日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

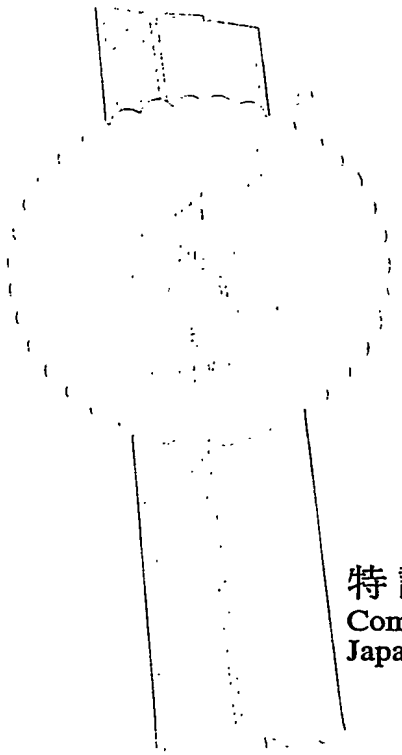
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　４月　１日

出願番号
Application Number: 特願２００３－０９８５９６

[ST. 10/C]: [ＪＰ２００３－０９８５９６]

出願人
Applicant(s): 松下電器産業株式会社



２００４年　４月１５日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００４－３０３１７８６

【書類名】　特許願
【整理番号】　2054051019
【あて先】　特許庁長官殿
【国際特許分類】　H04L 9/00
G07C 3/00
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　吉田　順二
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　▲浜▼井　信二
【特許出願人】
【識別番号】　000005821
【氏名又は名称】　松下電器産業株式会社
【代理人】
【識別番号】　100109210
【弁理士】
【氏名又は名称】　新居　広守
【手数料の表示】
【予納台帳番号】　049515
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　0213583
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　サーバ認証装置、認証装置およびダウンロードサーバの運用方法、媒体及び情報集合体

【特許請求の範囲】

【請求項１】　あるアプリケーションサーバが正当であることを保証し認証局が発行するサーバ証明書が正当であることを認証するためのＣＡ証明書と、次回更新用アドレスと、前記ＣＡ証明書と前記次回更新用アドレスの正当性を示す署名とを少なくとも有し、前記認証局が発行するＣＡ情報を、内部に保存するためのメモリと、

前記署名の認証を行うためのダウンロード公開鍵を保存するダウンロード公開鍵用メモリと、

前記認証局に関連するダウンロードサーバに接続し、前記ＣＡ情報を前記ダウンロードサーバから取得し、前記メモリに保存するＣＡ情報更新手段と、

前記アプリケーションサーバから前記サーバ証明書を取得し、前記メモリに保存されている前記ＣＡ情報内の前記ＣＡ証明書で、前記サーバ証明書の正当性を判断するサーバ証明書認証手段とを有し、

初期状態では、前記メモリには最初の前記ＣＡ情報が保存され、

前記ＣＡ情報更新手段は、前記ＣＡ証明書を更新する必要があれば、前記更新用アドレスが指定する前記ダウンロードサーバから新しいＣＡ情報を取得し、前記ＣＡ情報に含まれる前記署名を前記ダウンロード公開鍵で認証し、前記ＣＡ情報が正当であると証明できた場合には、前記ＣＡ情報を前記メモリに保存することを特徴とするサーバ認証装置。

【請求項２】　前記ダウンロードサーバは、少なくとも鍵情報を含み、前記メモリに保存されている前記ＣＡ情報内の前記ＣＡ証明書を用いることで前記ダウンロードサーバが正当であることを証明可能なＤＬサーバ証明書を保有しており、

前記ＣＡ情報更新手段は、前記ダウンロードサーバ接続時に、まず前記ＤＬサーバ証明書を取得し、前記メモリに保存されている前記ＣＡ情報内の前記ＣＡ証明書で認証を行い、前記ＤＬサーバ証明書の正当性を証明できた場合には、前記

ＤＬサーバ証明書に含まれる前記鍵情報を用いた秘密通信を行うことによって前記ダウンロードサーバから前記新しいＣＡ情報を取得し、

前記ＣＡ情報更新手段は、前記ＤＬサーバ証明書の正当性を証明できなかった場合には前記ダウンロードサーバとの接続を中断し、前記新しいＣＡ情報の取得を行わないことを特徴とする請求項１記載のサーバ認証装置。

【請求項３】　新しく取得したＣＡ情報に記載されている前記更新用アドレスは、前記ＣＡ情報の取得先である前記ダウンロードサーバではなく、別の認証局が発行する新しいＣＡ情報をダウンロードできるダウンロードサーバを示すアドレスであることを特徴とする請求項２記載のサーバ認証装置。

【請求項４】　あるアプリケーションサーバが正当であることを保証し、認証局が発行するサーバ証明書が正当であることを認証するためのＣＡ証明書と、次回更新用アドレスと、前記ＣＡ証明書と前記次回更新用アドレスの正当性を示す署名とを少なくとも有するＣＡ情報を、内部に保存するための第１のメモリおよび第２のメモリと、

前記認証局に関連するダウンロードサーバに接続し、前記ＣＡ情報を前記ダウンロードサーバから取得し、前記第１のメモリもしくは前記第２のメモリに保存するＣＡ情報更新手段と、

前記アプリケーションサーバから前記サーバ証明書を取得し、前記第１のメモリに保存されている前記ＣＡ情報内の前記認証鍵で、前記サーバ証明書の正当性を判断するサーバ証明書認証手段とを有し、

初期状態では、前記第１のメモリには最初の前記ＣＡ情報が保存され、また前記第２のメモリには何も保存されておらず、

前記ＣＡ情報更新手段は、ある期間ごとに前記第１のメモリに保存されている前記ＣＡ情報内の前記次回更新用アドレスで指定されるダウンロードサーバに接続を試みて、もし前記ダウンロードサーバに接続できた場合には、前記ダウンロードサーバから新しいＣＡ情報を取得し、前記新しいＣＡ情報に含まれる前記署名を前記ダウンロード公開鍵で認証し、前記新しいＣＡ情報が正当であると証明できた場合には、前記新しいＣＡ情報を前記第２のメモリに保存し、

前記サーバ証明書認証手段は、前記アプリケーションサーバから取得した前記

サーバ証明書を、前記第１のメモリに保存されている前記ＣＡ情報内の前記ＣＡ証明書を用いて正しく認証できなかった場合には、前記第１のメモリに保存されている前記ＣＡ情報内の前記ＣＡ証明書の代わりに、前記第２のメモリに保存されている前記ＣＡ情報内の前記ＣＡ証明書を用いて前記サーバ証明書の認証を行い、もし前記第２のメモリに保存されている前記ＣＡ情報内の前記ＣＡ証明書を用いて前記サーバ証明書の正当性が証明できた場合には、それ以降前記第２のメモリに保存されている前記ＣＡ情報を前記サーバ証明書の認証に用い、かつ第１のメモリに保存されている前記ＣＡ情報を削除し、以降は前記第１のメモリと、前記第２のメモリの役割を入れ替えて実行することを特徴とするサーバ認証装置。

【請求項５】　前記サーバ証明書認証手段は、前記アプリケーションサーバから取得した前記サーバ証明書を、前記第１のメモリに保存されている前記ＣＡ情報内の前記ＣＡ証明書を用いて正しく認証できなかった場合には、前記第２のメモリに保存されている前記ＣＡ情報内の前記ＣＡ証明書を用いて前記サーバ証明書の認証を行う代わりに、前記第２のメモリに保存されている前記ＣＡ情報を前記第１のメモリにコピーし、かつ前記第２のメモリに保存されている前記ＣＡ情報を削除した後、再度前記サーバ証明書の認証を行うことを特徴とする請求項４記載のサーバ認証装置。

【請求項６】　前記ダウンロードサーバは、少なくとも鍵情報を含み、前記第１のメモリに保存されている前記ＣＡ情報内の前記ＣＡ証明書を用いることで前記ダウンロードサーバが正当であることを証明するＤＬサーバ証明書を保有しており、

前記ＣＡ情報更新手段は、前記ダウンロードサーバ接続時に、まず前記ＤＬサーバ証明書を取得し、前記第１のメモリに保存されている前記ＣＡ情報内の前記ＣＡ証明書で認証を行い、前記ＤＬサーバ証明書の正当性を証明できた場合には、前記ＤＬサーバ証明書に含まれる前記鍵情報を用いた秘密通信を行うことによって前記ダウンロードサーバから前記新しいＣＡ情報を取得し、

前記ＣＡ情報更新手段は、前記ＤＬサーバ証明書の正当性を証明できなかった場合には前記ダウンロードサーバとの接続を中断し、前記新しいＣＡ情報の取得

を行わないことを特徴とする請求項４または５記載のサーバ認証装置。

【請求項７】　新しく取得したＣＡ情報に記載されている前記更新用アドレスは、前記ＣＡ情報の取得先である前記ダウンロードサーバではなく、別の認証局が発行する新しいＣＡ情報をダウンロードできるダウンロードサーバを示すアドレスであることを特徴とする請求項６記載のサーバ認証装置。

【請求項８】　あるアプリケーションサーバが正当であることを保証し、認証局が発行するサーバ証明書が正当であることを認証するためのＣＡ証明書と、次回更新用アドレスと、前記ＣＡ証明書と前記次回更新用アドレスの正当性を示す署名とを少なくとも有するＣＡ情報を、内部に保存するための第１のメモリと、

前記認証局に関連するダウンロードサーバに接続し、前記ＣＡ情報を前記ダウンロードサーバから取得し、前記第１のメモリに保存するＣＡ情報更新手段と、

前記アプリケーションサーバから前記サーバ証明書を取得し、前記第１のメモリに保存されている前記ＣＡ情報内の前記認証鍵で、前記サーバ証明書の正当性を判断するサーバ証明書認証手段とを有し、

初期状態では、前記第１のメモリには最初の前記ＣＡ情報が保存されており、

前記サーバ証明書認証手段は、前記アプリケーションサーバから取得した前記サーバ証明書を、前記第１のメモリに保存されている前記ＣＡ情報内の前記ＣＡ証明書を用いて正しく認証できなかった場合には、前記ＣＡ情報更新手段に更新指示を送り、

前記ＣＡ情報更新手段は、前記ＣＡ情報更新手段から前記更新指示を受け取ると、前記第１のメモリに保存されている前記ＣＡ情報内の前記次回更新用アドレスで指定されるダウンロードサーバに接続を試みて、もし前記ダウンロードに接続できた場合には、前記ダウンロードサーバから新しいＣＡ情報を取得し、前記新しいＣＡ情報に含まれる前記署名を前記ダウンロード公開鍵で認証し、前記新しいＣＡ情報が正当であると証明できた場合には、前記新しいＣＡ情報を前記第１のメモリに保存することを特徴とするサーバ認証装置。

【請求項９】さらに前記ＣＡ情報を保存するための第２のメモリを保有し、

前記第２のメモリは、初期状態には何も保存されておらず、

前記サーバ証明書認証手段は、前記アプリケーションサーバから取得した前記

サーバ証明書を、前記第１のメモリに保存されている前記ＣＡ情報内の前記ＣＡ証明書を用いて正しく認証できず、かつ前記第２のメモリに何も保存されていなかった場合には、前記ＣＡ情報更新手段に更新指示を送り、

前記ＣＡ情報更新手段は、取得した前記新しいＣＡ情報を前記第１のメモリの代わりに前記第２のメモリに保存し、

前記サーバ証明書認証手段は、前記新しいＣＡ情報が前記第２のメモリに保存されると、前記第２のメモリに保存されている前記新しいＣＡ情報内の前記ＣＡ証明書を用いて前記サーバ証明書の正当性が証明できた場合には、それ以降前記第２のメモリに保存されている前記ＣＡ情報を前記サーバ証明書の認証に用い、かつ第１のメモリに保存されている前記ＣＡ情報を削除し、以降は前記第１のメモリと、前記第２のメモリの役割を入れ替えて実行することを特徴とする請求項８記載のサーバ認証装置。

【請求項１０】　前記サーバ証明書認証手段は、前記第２のメモリに保存されている前記ＣＡ情報内の前記ＣＡ証明書を用いて前記サーバ証明書の認証を行う代わりに、前記第２のメモリに保存されている前記ＣＡ情報を前記第１のメモリにコピーし、かつ前記第２のメモリに保存されている前記ＣＡ情報を削除した後、再度前記サーバ証明書の認証を行うことを特徴とする請求項９記載のサーバ認証装置。

【請求項１１】　前記ダウンロードサーバは、少なくとも鍵情報を含み、前記第１のメモリに保存されている前記ＣＡ情報内の前記ＣＡ証明書を用いることで前記ダウンロードサーバが正当であることを証明するＤＬサーバ証明書を保有しており、

前記ＣＡ情報更新手段は、前記ダウンロードサーバ接続時に、まず前記ＤＬサーバ証明書を取得し、前記第１のメモリに保存されている前記ＣＡ情報内の前記ＣＡ証明書で認証を行い、前記ＤＬサーバ証明書の正当性を証明できた場合には、前記ＤＬサーバ証明書に含まれる前記鍵情報を用いた秘密通信を行うことによって前記ダウンロードサーバから前記新しいＣＡ情報を取得し、

前記ＣＡ情報更新手段は、前記ＤＬサーバ証明書の正当性を証明できなかった場合には前記ダウンロードサーバとの接続を中断し、前記新しいＣＡ情報の取得

を行わないことを特徴とする請求項８または９または１０記載のサーバ認証装置。

【請求項１２】　新しく取得したＣＡ情報に記載されている前記更新用アドレスは、前記ＣＡ情報の取得先である前記ダウンロードサーバではなく、別の認証局が発行する新しいＣＡ情報をダウンロードできるダウンロードサーバを示すアドレスであることを特徴とする請求項１１記載のサーバ認証装置。

【請求項１３】　請求項１～１２のいずれかに記載のサーバ認証装置の全部または一部の手段の全部または一部の機能をコンピュータにより実行させるためのプログラム及び／またはデータを担持した媒体であって、コンピュータにより処理可能なことを特徴とする媒体。

【請求項１４】　請求項１～１２のいずれかに記載のサーバ認証装置の全部または一部の手段の全部または一部の機能をコンピュータにより実行させるためのプログラム及び／またはデータであることを特徴とする情報集合体。

【請求項１５】　あるアプリケーションサーバが正当であることを保証するサーバ証明書を発行し、かつ前記サーバ証明書が正当であることを認証するためのＣＡ証明書と、次回更新用アドレスと、前記ＣＡ証明書と前記次回更新用アドレスの正当性を示す署名とを少なくとも含み、有効期間を持つＣＡ情報を発行し、かつ前記ＣＡ情報の正当性を証明する前記署名を作成するためのＤＬ秘密鍵を保有する認証局の機能を持つ認証装置と、

保有している前記ＣＡ情報を用いて前記アプリケーションサーバの前記証明書の正当性を証明するサーバ認証装置からの要求に応じ、前記ＣＡ情報に前記署名を含めて前記サーバ認証装置に送信するダウンロードサーバとにおける認証装置およびダウンロードサーバの運用方法であって、

有効期間がＴＣ１であり、かつ次回更新アドレスは第２のダウンロードサーバを示すアドレスである第１のＣＡ情報を発行する第１の認証装置を稼働させるステップと、

以降、Ｎ≧１である整数Ｎに対し、

第ＮのＣＡ情報の有効期間が終了するより期間ＴＤＮ（ＴＣＮ＞ＴＤＮ）だけ前の時点で、有効期間がＴＣ（Ｎ＋１）であり、かつ次回更新アドレスは第（Ｎ

＋２）のダウンロードサーバを示すアドレスである第（Ｎ＋１）のＣＡ情報、および前記第（Ｎ＋１）のＣＡ情報内のＣＡ証明書で認証可能なサーバ証明書を発行する第（Ｎ＋１）の認証装置を稼働させるステップと、

前記第（Ｎ＋１）の認証装置の稼働と同時に、前記サーバ認証装置からの要求に応じ、前記第（Ｎ＋１）のＣＡ情報を前記サーバ認証装置に送信する第（Ｎ＋１）のダウンロードサーバを稼働させるステップと、

第ＮのＣＡ情報の有効期間が終了すると、前記第Ｎの認証装置を終了するステップと

本来の第ＮのＣＡ情報の有効期間が終了する時点で、前記第（Ｎ＋１）のダウンロードサーバの稼働を終了するステップとを繰り返す、認証装置およびダウンロードサーバの運用方法。

【請求項１６】　さらに、

第ＮのＣＡ情報の有効期間が残りＴＤＮになる以前に、前記第ＮのＣＡ情報を無効にする必要が発生し、かつその時点で前記第（Ｎ＋１）の認証装置および前記第（Ｎ＋１）のダウンロードサーバが稼働していない場合には、

有効期間をＴＣ（Ｎ＋１）とし、かつ次回更新アドレスは第（Ｎ＋２）のダウンロードサーバを示すアドレスである第（Ｎ＋１）のＣＡ情報を発行する第（Ｎ＋１）の認証装置をその時点で稼働させるステップと、

第（Ｎ＋１）の認証装置の稼働と同時に前記第（Ｎ＋１）のＣＡ情報を前記サーバ認証装置に送信する第（Ｎ＋１）のダウンロードサーバを稼働させるステップと、

第（Ｎ＋１）の認証装置の稼働と同時に前記第Ｎの認証装置の稼働を終了し、前記第ＮのＣＡ情報を無効にするステップとを実行し、

第ＮのＣＡ情報の有効期間が残りＴＤＮになる以前に、前記第ＮのＣＡ情報を無効にする必要が発生し、かつ前記第（Ｎ＋１）の認証装置および前記第（Ｎ＋１）のダウンロードサーバがすでに稼働している場合には、

その時点で前記第Ｎの認証装置の稼働を終了し、前記第ＮのＣＡ情報を無効にするステップとを実行することを特徴とする請求項１５記載の認証装置およびダウンロードサーバの運用方法。

【請求項１７】　前記第Ｎのダウンロードサーバは、少なくとも第Ｎの鍵情報を含み、前記第Ｎのダウンロードサーバが正当であることを証明する第ＮのＤＬサーバ証明書を保有しており、かつ前記サーバ認証装置の要求に応じて前記第ＮのＤＬサーバ証明書を送信し、

かつ前記第Ｎの鍵情報を用いた秘密通信によって、前記サーバ認証装置に第ＮのＣＡ情報を送信することを特徴とする請求項１５または請求項１６に記載の認証装置およびダウンロードサーバの運用方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、認証局よって発行されるサーバ証明書の正当性を認証するためのＣＡ情報が有効期間切れなどのために失効する場合に、安全かつ確実に新しいＣＡ情報を更新できるサーバ認証装置、認証局およびダウンロードサーバの運用方法、媒体及び情報集合体に関するものである。

【０００２】

【従来の技術】

近年、インターネットは急速に普及、拡大し、電子メールやインターネットショッピングなど様々なサービスが提供されている。しかし、その一方で個人情報など、インターネットを通して通信されるデータの盗聴や改ざんなどの問題も発生してきた。そうした悪意ある第３者からの攻撃を防ぐために、様々なセキュリティ技術が考案、導入されてきた。　セキュリティ技術としては、例えば通信データが途中で盗聴されても内容を分からないようにする暗号や、通信データが途中で改ざんされていないかを検証できる認証などが挙げられる。

【０００３】

こうした技術を利用し、インターネットでよく用いられているセキュリティ技術にＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔｓ　Ｌａｙｅｒ）と呼ばれる方式がある。ＳＳＬは、特許文献１で提案されており、サーバが正当であること、通信において通信データの内容が漏洩していないこと、かつ受信するクライアントが受け取った通信データの内容が途中で改ざんされていないことの３つを保証する通

信を提供する方式である。

【０００４】

ＳＳＬにおける通信方式の概要を、図８および図９を用いて説明する。

【０００５】

図８は、ＳＳＬにおける鍵情報および証明書の準備を表す図である。図８において、１０１は認証局、１０２はクライアント、１０３はサーバ、１０４はＣＡ公開鍵、１０５はＣＡ秘密鍵、１０６はＣＡ証明書、１０７はサーバ公開鍵、１０８はサーバ秘密鍵、１０９はサーバ証明書、１１０は署名である。

【０００６】

図９は、ＳＳＬにおける通信プロトコルを表す図である。図９において、２０１は通信共通鍵である。

【０００７】

認証局１０１は、あらかじめＣＡ公開鍵１０４とＣＡ秘密鍵１０５のペアを生成し、同時にＣＡ公開鍵１０４や認証局１０１に関する情報を記載したＣＡ証明書１０６を作成する。

【０００８】

サーバ１０３は、稼働前にまずサーバ公開鍵１０７とサーバ秘密鍵のペアを生成する。サーバ１０３は、サーバ公開鍵１０７とサーバ１０３に関する情報を認証局１０１に送信し、サーバ証明書１０９の発行を依頼する。

【０００９】

認証局１０１は、ＣＡ秘密鍵１０５を用いて、サーバ１０３から受け取った情報やその他必要な情報から署名１１０を作成し、サーバ１０３から受け取った情報やその他必要な情報および署名１１０を合わせたものをサーバ証明書１０９として、サーバ１０３に発行する。

【００１０】

サーバ１０３は受け取ったサーバ証明書１０９を保存しておく。

【００１１】

またクライアント１０２は、あらかじめ認証局１０１からＣＡ証明書１０６を取得し、保存しておく。

【００１２】

実際にクライアント１０２とサーバ１０３の間で秘密通信は以下のように行われる。

【００１３】

クライアント１０２はサーバ１０３に接続すると、まず秘密通信で用いる暗号化方式の仕様を相互に確認する。

【００１４】

次にサーバ１０３はクライアント１０２にサーバ証明書１０９を送付する。

【００１５】

クライアント１０２は、内部に保存しているＣＡ公開鍵１０４を用いてサーバ証明書１０９が正当であるかどうかを確認する。もしサーバ証明書１０９が正当、すなわちサーバ証明書１０９に含まれている署名１１０がＣＡ秘密鍵１０５で署名されたものであれば、クライアント１０２はＣＡ公開鍵１０４を用いて検証すれば、サーバ証明書１０９が正当であることが確認できる。

【００１６】

クライアント１０２は、サーバ証明書１０９が正当であると確認すると、クライアント側共通鍵生成情報をランダムに作成し、サーバ１０３に送付する。

【００１７】

サーバ１０３は、サーバ側共通鍵生成情報をランダムに作成し、クライアント１０２に送付する。

【００１８】

サーバ１０３およびクライアント１０２は、サーバ側共通鍵生成情報およびクライアント側共通鍵生成情報を用いて、通信用共通鍵２０１を生成する。

【００１９】

これにより、クライアント１０２とサーバ１０３で通信用共通鍵２０１を共有することができる。

【００２０】

以降、クライアント１０２およびサーバ１０３は、通信用共通鍵２０１を用いて、通信するデータの暗号化および復号を行うことで、秘密通信を行うことが可

能となる。

【００２１】

なお、ＣＡ証明書１０６やサーバ証明書１０９のフォーマットとしては、ＩＴＵ－Ｔ（国際電気通信連合）で定義されたＸ．５０９証明書を用いることが多い。

【００２２】

さて、Ｘ．５０９証明書においては、サーバ証明書１０９には有効期限を設けるようになっている。というのも、秘密鍵の安全性は、公開鍵や通信データから秘密鍵を計算するときにかかる時間が十分に長いことに依存しており、同じ鍵を長期間使用していると、その分秘密鍵が暴露される可能性が高くなるためである。

【００２３】

同様にＣＡ証明書１０６にも有効期限を設けるが、一般にサーバ証明書１０９より長い期間が設定されている。

【００２４】

ところで、ＣＡ証明書の有効期限が切れた場合、もしくは何らかの原因でＣＡ秘密鍵が暴露されてしまった場合には、速やかに新しい鍵ペアを作成し、新しいＣＡ証明書を発行もしくは取得しなければならない。

【００２５】

例えば、十分な数の認証局が同時に存在し、クライアントがＰＣ（パーソナルコンピュータ）のように、十分な計算機リソースを保有しており、それらのＣＡ証明書を全てもしくは十分な数だけ保有可能な場合は、サーバは失効した認証局の代わりに別の認証局から取得したサーバ証明書を使用することが可能である。クライアントは、保有しているＣＡ証明書を順番に用いてサーバ証明書の認証を行い、いずれかのＣＡ証明書でサーバ証明書の正当性を確認できれば、そのサーバは正当であると確認できる。

【００２６】

また新しい認証局ができ、そのＣＡ証明書を取得するためには、例えば認証局自身かもしくは信頼できるサーバなどから、クライアントのユーザが取得し、ユ

ーザが自分でクライアントにインストールするなどして実行できる。

【００２７】

またサーバ証明書の有効期限が間近になった場合や、サーバ証明書が失効した場合に、自動的に新しいサーバ証明書を更新する装置および方法が、例えば特許文献２や特許文献３に記載されている。

【００２８】

【特許文献１】

Ｕ．Ｓ．Ｐａｔｅｎｔ　５６５７３９０

【００２９】

【特許文献２】

特開２００１－１９７０５４号公報

【００３０】

【特許文献３】

特開２００２－２１５８２６号公報

【００３１】

【発明が解決しようとする課題】

しかしながら、家電製品などのように十分なリソースを保有していないクライアントの場合には、常に多数個のＣＡ証明書を保有したり、複数のＣＡ証明書を用いて検証するプログラムもしくは回路を組み込むことが困難であるという問題点が生じる。

【００３２】

また、時計を保有していなかったり、あるいは時計を正確な時刻に設定する手段を持たないクライアントの場合には、ＣＡ証明書の有効期限の判定が困難で、有効期限が近づくと新しいＣＡ証明書を自動的に更新することができないという問題点がある。

【００３３】

本発明は、このような従来の問題点を鑑みてなされたものであって、リソースが少ないクライアントであっても、安全かつ確実にＣＡ証明書を更新することができるサーバ認証装置、認証局およびダウンロードサーバの運用方法、媒体及び

情報集合体を提供することを目的とするものである。

【００３４】

【課題を解決するための手段】

上述した課題を解決するために、第１の本発明（請求項１に対応）は、あるアプリケーションサーバが正当であることを保証し、認証局が発行するサーバ証明書が正当であることを認証するためのＣＡ証明書と、次回更新用アドレスと、前記ＣＡ証明書と前記次回更新用アドレスの正当性を示す署名とを少なくとも有し、前記認証局が発行するＣＡ情報を、内部に保存するためのメモリと、前記署名の認証を行うためのダウンロード公開鍵を保存するダウンロード公開鍵用メモリと、前記認証局に関連するダウンロードサーバに接続し、前記ＣＡ情報を前記ダウンロードサーバから取得し、前記メモリに保存するＣＡ情報更新手段と、前記アプリケーションサーバから前記サーバ証明書を取得し、前記メモリに保存されている前記ＣＡ情報内の前記ＣＡ証明書で、前記サーバ証明書の正当性を判断するサーバ証明書認証手段とを有し、初期状態では、前記メモリには最初の前記ＣＡ情報が保存され、前記ＣＡ情報更新手段は、前記ＣＡ証明書を更新する必要があれば、前記更新用アドレスが指定する前記ダウンロードサーバから新しいＣＡ情報を取得し、前記ＣＡ情報に含まれる前記署名を前記ダウンロード公開鍵で認証し、前記ＣＡ情報が正当であると証明できた場合には、前記ＣＡ情報を前記メモリに保存することを特徴とするサーバ認証装置である。

【００３５】

第２の本発明（請求項２に対応）は、前記ダウンロードサーバは、少なくとも鍵情報を含み、前記メモリに保存されている前記ＣＡ情報内の前記ＣＡ証明書を用いることで前記ダウンロードサーバが正当であることを証明可能なＤＬサーバ証明書を保有しており、前記ＣＡ情報更新手段は、前記ダウンロードサーバ接続時に、まず前記ＤＬサーバ証明書を取得し、前記メモリに保存されている前記ＣＡ情報内の前記ＣＡ証明書で認証を行い、前記ＤＬサーバ証明書の正当性を証明できた場合には、前記ＤＬサーバ証明書に含まれる前記鍵情報を用いた秘密通信を行うことによって前記ダウンロードサーバから前記新しいＣＡ情報を取得し、前記ＣＡ情報更新手段は、前記ＤＬサーバ証明書の正当性を証明できなかった場

合には前記ダウンロードサーバとの接続を中断し、前記新しいＣＡ情報の取得を行わないことを特徴とする第１の本発明に記載のサーバ認証装置である。

【００３６】

第３の本発明（請求項３に対応）は、新しく取得したＣＡ情報に記載されている前記更新用アドレスは、前記ＣＡ情報の取得先である前記ダウンロードサーバではなく、別の認証局が発行する新しいＣＡ情報をダウンロードできるダウンロードサーバを示すアドレスであることを特徴とする第２の本発明に記載のサーバ認証装置である。

【００３７】

第４の本発明（請求項４に対応）は、あるアプリケーションサーバが正当であることを保証し、認証局が発行するサーバ証明書が正当であることを認証するためのＣＡ証明書と、次回更新用アドレスと、前記ＣＡ証明書と前記次回更新用アドレスの正当性を示す署名とを少なくとも有するＣＡ情報を、内部に保存するための第１のメモリおよび第２のメモリと、前記認証局に関連するダウンロードサーバに接続し、前記ＣＡ情報を前記ダウンロードサーバから取得し、前記第１のメモリもしくは前記第２のメモリに保存するＣＡ情報更新手段と、前記アプリケーションサーバから前記サーバ証明書を取得し、前記第１のメモリに保存されている前記ＣＡ情報内の前記認証鍵で、前記サーバ証明書の正当性を判断するサーバ証明書認証手段とを有し、初期状態では、前記第１のメモリには最初の前記ＣＡ情報が保存され、また前記第２のメモリには何も保存されておらず、前記ＣＡ情報更新手段は、ある期間ごとに前記第１のメモリに保存されている前記ＣＡ情報内の前記次回更新用アドレスで指定されるダウンロードサーバに接続を試みて、もし前記ダウンロードサーバに接続できた場合には、前記ダウンロードサーバから新しいＣＡ情報を取得し、前記新しいＣＡ情報に含まれる前記署名を前記ダウンロード公開鍵で認証し、前記新しいＣＡ情報が正当であると証明できた場合には、前記新しいＣＡ情報を前記第２のメモリに保存し、前記サーバ証明書認証手段は、前記アプリケーションサーバから取得した前記サーバ証明書を、前記第１のメモリに保存されている前記ＣＡ情報内の前記ＣＡ証明書を用いて正しく認証できなかった場合には、前記第１のメモリに保存されている前記ＣＡ情報内の

前記ＣＡ証明書の代わりに、前記第２のメモリに保存されている前記ＣＡ情報内の前記ＣＡ証明書を用いて前記サーバ証明書の認証を行い、もし前記第２のメモリに保存されている前記ＣＡ情報内の前記ＣＡ証明書を用いて前記サーバ証明書の正当性が証明できた場合には、それ以降前記第２のメモリに保存されている前記ＣＡ情報を前記サーバ証明書の認証に用い、かつ第１のメモリに保存されている前記ＣＡ情報を削除し、以降は前記第１のメモリと、前記第２のメモリの役割を入れ替えて実行することを特徴とするサーバ認証装置である。

【００３８】

第５の本発明（請求項５に対応）は、前記サーバ証明書認証手段は、前記アプリケーションサーバから取得した前記サーバ証明書を、前記第１のメモリに保存されている前記ＣＡ情報内の前記ＣＡ証明書を用いて正しく認証できなかった場合には、前記第２のメモリに保存されている前記ＣＡ情報内の前記ＣＡ証明書を用いて前記サーバ証明書の認証を行う代わりに、前記第２のメモリに保存されている前記ＣＡ情報を前記第１のメモリにコピーし、かつ前記第２のメモリに保存されている前記ＣＡ情報を削除した後、再度前記サーバ証明書の認証を行うことを特徴とする第４の本発明に記載のサーバ認証装置である。。

【００３９】

第６の本発明（請求項６に対応）は、前記ダウンロードサーバは、少なくとも鍵情報を含み、前記第１のメモリに保存されている前記ＣＡ情報内の前記ＣＡ証明書を用いることで前記ダウンロードサーバが正当であることを証明するＤＬサーバ証明書を保有しており、前記ＣＡ情報更新手段は、前記ダウンロードサーバ接続時に、まず前記ＤＬサーバ証明書を取得し、前記第１のメモリに保存されている前記ＣＡ情報内の前記ＣＡ証明書で認証を行い、前記ＤＬサーバ証明書の正当性を証明できた場合には、前記ＤＬサーバ証明書に含まれる前記鍵情報を用いた秘密通信を行うことによって前記ダウンロードサーバから前記新しいＣＡ情報を取得し、前記ＣＡ情報更新手段は、前記ＤＬサーバ証明書の正当性を証明できなかった場合には前記ダウンロードサーバとの接続を中断し、前記新しいＣＡ情報の取得を行わないことを特徴とする第４または第５の本発明に記載のサーバ認証装置である。

【００４０】

第７の本発明（請求項７に対応）は、新しく取得したＣＡ情報に記載されている前記更新用アドレスは、前記ＣＡ情報の取得先である前記ダウンロードサーバではなく、別の認証局が発行する新しいＣＡ情報をダウンロードできるダウンロードサーバを示すアドレスであることを特徴とする第６の本発明に記載のサーバ認証装置である。

【００４１】

第８の本発明（請求項８に対応）は、あるアプリケーションサーバが正当であることを保証し、認証局が発行するサーバ証明書が正当であることを認証するためのＣＡ証明書と、次回更新用アドレスと、前記ＣＡ証明書と前記次回更新用アドレスの正当性を示す署名とを少なくとも有するＣＡ情報を、内部に保存するための第１のメモリと、前記認証局に関連するダウンロードサーバに接続し、前記ＣＡ情報を前記ダウンロードサーバから取得し、前記第１のメモリに保存するＣＡ情報更新手段と、前記アプリケーションサーバから前記サーバ証明書を取得し、前記第１のメモリに保存されている前記ＣＡ情報内の前記認証鍵で、前記サーバ証明書の正当性を判断するサーバ証明書認証手段とを有し、初期状態では、前記第１のメモリには最初の前記ＣＡ情報が保存されており、前記サーバ証明書認証手段は、前記アプリケーションサーバから取得した前記サーバ証明書を、前記第１のメモリに保存されている前記ＣＡ情報内の前記ＣＡ証明書を用いて正しく認証できなかった場合には、前記ＣＡ情報更新手段に更新指示を送り、前記ＣＡ情報更新手段は、前記ＣＡ情報更新手段から前記更新指示を受け取ると、前記第１のメモリに保存されている前記ＣＡ情報内の前記次回更新用アドレスで指定されるダウンロードサーバに接続を試みて、もし前記ダウンロードに接続できた場合には、前記ダウンロードサーバから新しいＣＡ情報を取得し、前記新しいＣＡ情報に含まれる前記署名を前記ダウンロード公開鍵で認証し、前記新しいＣＡ情報が正当であると証明できた場合には、前記新しいＣＡ情報を前記第１のメモリに保存することを特徴とするサーバ認証装置である。

【００４２】

第９の本発明（請求項９に対応）は、さらに前記ＣＡ情報を保存するための第

２のメモリを保有し、前記第２のメモリは、初期状態には何も保存されておらず、前記サーバ証明書認証手段は、前記アプリケーションサーバから取得した前記サーバ証明書を、前記第１のメモリに保存されている前記ＣＡ情報内の前記ＣＡ証明書を用いて正しく認証できず、かつ前記第２のメモリに何も保存されていなかった場合には、前記ＣＡ情報更新手段に更新指示を送り、前記ＣＡ情報更新手段は、取得した前記新しいＣＡ情報を前記第１のメモリの代わりに前記第２のメモリに保存し、前記サーバ証明書認証手段は、前記新しいＣＡ情報が前記第２のメモリに保存されると、前記第２のメモリに保存されている前記新しいＣＡ情報内の前記ＣＡ証明書を用いて前記サーバ証明書の正当性が証明できた場合には、それ以降前記第２のメモリに保存されている前記ＣＡ情報を前記サーバ証明書の認証に用い、かつ第１のメモリに保存されている前記ＣＡ情報を削除し、以降は前記第１のメモリと、前記第２のメモリの役割を入れ替えて実行することを特徴とする第８の本発明に記載のサーバ認証装置である。

【００４３】

第１０の本発明（請求項１０に対応）は、前記サーバ証明書認証手段は、前記第２のメモリに保存されている前記ＣＡ情報内の前記ＣＡ証明書を用いて前記サーバ証明書の認証を行う代わりに、前記第２のメモリに保存されている前記ＣＡ情報を前記第１のメモリにコピーし、かつ前記第２のメモリに保存されている前記ＣＡ情報を削除した後、再度前記サーバ証明書の認証を行うことを特徴とする第９の本発明に記載のサーバ認証装置である。

【００４４】

第１１の本発明（請求項１１に対応）は、前記ダウンロードサーバは、少なくとも鍵情報を含み、前記第１のメモリに保存されている前記ＣＡ情報内の前記ＣＡ証明書を用いることで前記ダウンロードサーバが正当であることを証明するＤＬサーバ証明書を保有しており、前記ＣＡ情報更新手段は、前記ダウンロードサーバ接続時に、まず前記ＤＬサーバ証明書を取得し、前記第１のメモリに保存されている前記ＣＡ情報内の前記ＣＡ証明書で認証を行い、前記ＤＬサーバ証明書の正当性を証明できた場合には、前記ＤＬサーバ証明書に含まれる前記鍵情報を用いた秘密通信を行うことによって前記ダウンロードサーバから前記新しいＣＡ

情報を取得し、前記ＣＡ情報更新手段は、前記ＤＬサーバ証明書の正当性を証明できなかった場合には前記ダウンロードサーバとの接続を中断し、前記新しいＣＡ情報の取得を行わないことを特徴とする第８から第１０のいずれかの本発明に記載のサーバ認証装置である。

【００４５】

第１２の本発明（請求項１２に対応）は、新しく取得したＣＡ情報に記載されている前記更新用アドレスは、前記ＣＡ情報の取得先である前記ダウンロードサーバではなく、別の認証局が発行する新しいＣＡ情報をダウンロードできるダウンロードサーバを示すアドレスであることを特徴とする第１１の本発明に記載のサーバ認証装置である。

【００４６】

第１３の本発明（請求項１３に対応）は、第１から第１２の本発明のいずれかに記載のサーバ認証装置の全部または一部の手段の全部または一部の機能をコンピュータにより実行させるためのプログラム及び／またはデータを担持した媒体であって、コンピュータにより処理可能なことを特徴とする媒体である。

【００４７】

第１４の本発明（請求項１４に対応）は、第１から第１２の本発明のいずれかに記載のサーバ認証装置の全部または一部の手段の全部または一部の機能をコンピュータにより実行させるためのプログラム及び／またはデータであることを特徴とする情報集合体である。

【００４８】

第１５の本発明（請求項１５に対応）は、あるアプリケーションサーバが正当であることを保証するサーバ証明書を発行し、かつ前記サーバ証明書が正当であることを認証するためのＣＡ証明書と、次回更新用アドレスと、前記ＣＡ証明書と前記次回更新用アドレスの正当性を示す署名とを少なくとも含み、有効期間を持つＣＡ情報を発行し、かつ前記ＣＡ情報の正当性を証明する前記署名を作成するためのＤＬ秘密鍵を保有する認証局の機能を持つ認証装置と、保有している前記ＣＡ情報を用いて前記アプリケーションサーバの前記証明書の正当性を証明するサーバ認証装置からの要求に応じ、前記ＣＡ情報に前記署名を含めて前記サー

バ認証装置に送信するダウンロードサーバとにおける認証装置およびダウンロードサーバの運用方法であって、有効期間がＴＣ１であり、かつ次回更新アドレスは第２のダウンロードサーバを示すアドレスである第１のＣＡ情報を発行する第１の認証装置を稼働させるステップと、以降、Ｎ≧１である整数Ｎに対し、第ＮのＣＡ情報の有効期間が終了するより期間ＴＤＮ（ＴＣＮ＞ＴＤＮ）だけ前の時点で、有効期間がＴＣ（Ｎ＋１）であり、かつ次回更新アドレスは第（Ｎ＋２）のダウンロードサーバを示すアドレスである第（Ｎ＋１）のＣＡ情報、および前記第（Ｎ＋１）のＣＡ情報内のＣＡ証明書で認証可能なサーバ証明書を発行する第（Ｎ＋１）の認証装置を稼働させるステップと、前記第（Ｎ＋１）の認証装置の稼働と同時に、前記サーバ認証装置からの要求に応じ、前記第（Ｎ＋１）のＣＡ情報を前記サーバ認証装置に送信する第（Ｎ＋１）のダウンロードサーバを稼働させるステップと、第ＮのＣＡ情報の有効期間が終了すると、前記第Ｎの認証装置を終了するステップと、本来の第ＮのＣＡ情報の有効期間が終了する時点で、前記第（Ｎ＋１）のダウンロードサーバの稼働を終了するステップとを繰り返す、認証装置およびダウンロードサーバの運用方法である。

【００４９】

第１６の本発明（請求項１６に対応）は、さらに、第ＮのＣＡ情報の有効期間が残りＴＤＮになる以前に、前記第ＮのＣＡ情報を無効にする必要が発生し、かつその時点で前記第（Ｎ＋１）の認証装置および前記第（Ｎ＋１）のダウンロードサーバが稼働していない場合には、有効期間をＴＣ（Ｎ＋１）とし、かつ次回更新アドレスは第（Ｎ＋２）のダウンロードサーバを示すアドレスである第（Ｎ＋１）のＣＡ情報を発行する第（Ｎ＋１）の認証装置をその時点で稼働させるステップと、第（Ｎ＋１）の認証装置の稼働と同時に前記第（Ｎ＋１）のＣＡ情報を前記サーバ認証装置に送信する第（Ｎ＋１）のダウンロードサーバを稼働させるステップと、第（Ｎ＋１）の認証装置の稼働と同時に前記第Ｎの認証装置の稼働を終了し、前記第ＮのＣＡ情報を無効にするステップとを実行し、第ＮのＣＡ情報の有効期間が残りＴＤＮになる以前に、前記第ＮのＣＡ情報を無効にする必要が発生し、かつ前記第（Ｎ＋１）の認証装置および前記第（Ｎ＋１）のダウンロードサーバがすでに稼働している場合には、その時点で前記第Ｎの認証装置の

稼働を終了し、前記第ＮのＣＡ情報を無効にするステップとを実行することを特徴とする第１５の本発明に記載の認証装置およびダウンロードサーバの運用方法である。

【００５０】

第１７の本発明（請求項１７に対応）は、前記第Ｎのダウンロードサーバは、少なくとも第Ｎの鍵情報を含み、前記第Ｎのダウンロードサーバが正当であることを証明する第ＮのＤＬサーバ証明書を保有しており、かつ前記サーバ認証装置の要求に応じて前記第ＮのＤＬサーバ証明書を送信し、かつ前記第Ｎの鍵情報を用いた秘密通信によって、前記サーバ認証装置に第ＮのＣＡ情報を送信することを特徴とする第１５または第１６の本発明に記載の認証装置およびダウンロードサーバの運用方法。

【００５１】

【発明の実施の形態】

以下に、本発明の実施の形態を図面を参照して説明する。

【００５２】

（第１の実施の形態）

以下、本発明の第１の実施の形態について、図１および図２を用いて説明する。

図１は、ＣＡ情報の一例である。図１において、３０１はＣＡ情報、３０２は次回ダウンロードサーバのＵＲＬ、３０３はＣＡ署名である。

【００５３】

図２は、サーバ認証を行うクライアントの構成例である。図２において、１０１ａは認証局Ａ、１０１ｂは認証局Ｂ、１０５ａはＣＡ秘密鍵Ａ、１０５ｂはＣＡ秘密鍵Ｂ、１０６ａはＣＡ証明書Ａ、１０６ｂはＣＡ証明書Ｂ、３０１ａはＣＡ情報Ａ、３０１ｂはＣＡ情報Ｂ、３０２ｂはダウンロードサーバＢのＵＲＬ、３０２ｃはダウンロードサーバＣのＵＲＬ、３０３ａはＣＡ署名Ａ、３０３ｂはＣＡ署名Ｂ、４０１はアプリケーションサーバ、４０２ａはＡＰサーバ証明書Ａ、４０３ａはＡＰサーバ公開鍵Ａ、４０４ａはＡＰサーバ秘密鍵Ａ、４０５ａはＡＰ署名Ａ、４０６ｂはダウンロードサーバＢ、４０８ｂはＤＬサーバ証明書Ｂ

、４０９ｂはＤＬサーバ公開鍵Ｂ、４１０ｂはＤＬサーバ秘密鍵Ｂ、４１２ｂはＤＬ署名Ｂ、４１３はＤＬ秘密鍵、４１４はＤＬ公開鍵、４１５はクライアント、４１６はサーバ認証部、４１７はＣＡ情報更新部、４１８はメモリ、４１９は予備メモリである。

【００５４】

本実施の形態においては、ＣＡ情報３０１を発行し、かつアプリケーションサーバ４０１にＡＰサーバ証明書を発行する装置を、認証局と表記する。

【００５５】

クライアント４１５に渡す情報として、ＣＡ情報３０１を用意する。ＣＡ情報３０１には、図１に示すように、ＣＡ証明書１０６、ＣＡ証明書１０６の長さ、将来稼働し次回ＣＡ情報をダウンロードするためのダウンロードサーバのＵＲＬ３０２、ダウンロードサーバのＵＲＬの長さ、ＣＡ署名３０３が含まれている。ＣＡ署名３０３は、ＣＡ署名３０３以外の４つの情報に対して、ＤＬ秘密鍵４１３で署名を行ったものである。ＤＬ秘密鍵４１３は、ＤＬ公開鍵４１４とペアであり、ＤＬ公開鍵４１４を用いることでＣＡ署名３０３の正当性を調べることができる。

【００５６】

以下、クライアント４１５におけるサーバ認証動作について説明する。

まずアプリケーションサーバ４０１は、ＳＳＬ通信用の鍵ペアであるＡＰサーバ秘密鍵Ａ４０４ａとＡＰサーバ公開鍵Ａ４０３ａを作成し、ＡＰサーバ公開鍵Ａ４０３ａおよびその他の必要事項を認証局Ａ１０１ａに送付し、サーバ証明書の発行を依頼する。

【００５７】

認証局Ａ１０１ａは、あらかじめＣＡ秘密鍵Ａ１０５ａとＣＡ公開鍵Ａの鍵ペアを保有しており、アプリケーションサーバ４０１からサーバ証明書の発行依頼を受け取ると、ＣＡ秘密鍵Ａ１０５ａによる署名と共にＡＰサーバ証明書４０２ａを発行し、アプリケーションサーバ４０１に送付する。

【００５８】

また認証局Ａ１０１ａは、ＣＡ公開鍵Ａを含むサーバ証明書であるＣＡ証明書

Ａ１０６ａを作成し、同時にＣＡ証明書Ａ１０６ａを含むＣＡ情報Ａ３０１ａを作成する。ＣＡ情報Ａ３０１ａに付加するＵＲＬ３０２ｂは、ダウンロードサーバＢ４０６ｂのＵＲＬである。

【００５９】

クライアント４１５は、初期状態として、内部のメモリ４１８にＣＡ情報Ａ３０１ａを保存しており、予備メモリ４１９には何も保存していない。

【００６０】

クライアント４１５がアプリケーションサーバ４０１とＳＳＬ通信を行う場合には、サーバ認証部４１６はアプリケーションサーバ４０１からＡＰサーバ証明書４０２ａを取得し、メモリ４１８に保存しているＣＡ証明書Ａ１０６ａ内のＣＡ公開鍵Ａで認証を行うことができる。

【００６１】

ＡＰサーバ証明書４０２ａが正当であると証明されると、従来の技術で説明したように、クライアント４１５とアプリケーションサーバ４０１との間でＳＳＬ通信を行うことができるようになる。

【００６２】

次に、クライアント４１５におけるＣＡ情報の更新動作について説明する。

【００６３】

ＣＡ証明書Ａ１０６ａの有効期限が近づくと、クライアント４１５があらかじめ新しいＣＡ証明書を取得できるようにする必要がある。そのため、まずＣＡ証明書Ａ１０６ａの有効期限が来る前に、ＣＡ秘密鍵Ｂ１０５ｂとＣＡ公開鍵Ｂの鍵ペアを持つ新しい認証局Ｂ１０１ｂを立ち上げ、認証局Ｂ１０１ｂはＣＡ公開鍵Ｂを含む新しいＣＡ証明書Ｂ１０６ｂを作成する。ただしこの時点では、認証局Ｂ１０１ｂはアプリケーションサーバ４０１に対するＡＰサーバ証明書を発行しない。サーバ証明書を発行する場合には、この時点ではアプリケーションサーバ４０１は、クライアント４１５とのサーバ認証には、認証局Ｂ１０１ｂから取得したＡＰサーバ証明書は使用しない。

【００６４】

また認証局Ｂ１０１ｂは同時にＣＡ証明書Ｂ１０６ｂから新しいＣＡ情報Ｂ３

０１ｂを作成する。内部に記載するＵＲＬ３０２ｃは、次回に新しいＣＡ情報をダウンロードするためのダウンロードサーバＣのＵＲＬであり、ＣＡ署名Ｂ３０３ｂはＣＡ署名Ａ３０３ａと同様に作成したものである。

【００６５】

次に、ＵＲＬ３０２ｂで指定される場所にダウンロードサーバＢ４０６ｂを立ち上げ、ＣＡ情報Ｂ３０１ｂをダウンロードできるようにする。このとき、ダウンロードサーバＢ４０６ｂにおいても、ＤＬサーバ公開鍵４０９ｂとＤＬサーバ秘密鍵４１０ｂの鍵ペアを生成し、ＤＬサーバ公開鍵４０９ｂおよび必要事項を認証局Ａ１０１ａに送付し、認証局Ａ１０１ａからサーバ証明書としてＤＬサーバ証明書Ｂ４０８ｂを取得する。

【００６６】

さて、クライアント４１５のＣＡ情報更新部４１７は、メモリ４１８に保存しているＣＡ情報Ａ３０１ａに記載されているＵＲＬ３０２ｂが示すダウンロードサーバにある程度の期間、例えば１ヶ月毎に接続を試みる。ダウンロードサーバＢ４０６ｂが稼働していないときには、ＣＡ情報更新部４１７はダウンロードサーバＢ４０６ｂへの接続に失敗するので、この場合には更新する必要はないと判断する。その後１ヶ月後に同様に接続を試みる。

【００６７】

またダウンロードサーバＢ４０６ｂが稼働しているときには、ＣＡ情報更新部４１７はダウンロードサーバＢ４０６ｂへの接続に成功するので、まずＤＬサーバ証明書Ｂ４０８ｂを取得し、メモリ４１８に保存しているＣＡ公開鍵Ａを用いて認証を行う。

【００６８】

ＤＬサーバ証明書Ｂ４０８ｂの正当性が確認されると、次にＣＡ情報更新部４１７はダウンロードサーバＢ４０６ｂからＣＡ情報Ｂ３０１ｂを取得する。ＣＡ情報更新部４１７は、取得したＣＡ情報Ｂ３０１ｂ内のＣＡ署名Ｂ３０３ｂをＤＬ公開鍵４１４で認証し、ＣＡ情報Ｂ３０１ｂの正当性を確認できると、ＣＡ署名Ｂ３０３ｂを予備メモリ４１９に保存する。

【００６９】

次にＣＡ証明書１０６ａの有効期限が切れたときのアプリケーションサーバ４０１とクライアント４１５の動作について説明する。

【００７０】

アプリケーションサーバ４０１は、ＣＡ証明書１０６ａの有効期限が切れる前か、もしくは切れると同時に、ＡＰサーバ公開鍵とＡＰサーバ秘密鍵の新しい鍵ペアを生成し、認証局Ｂ１０１ｂから新しいＡＰサーバ証明書Ｂを取得する。アプリケーションサーバ４０１は、ＣＡ証明書１０６ａの有効期限が切れると、古いＡＰサーバ証明書Ａ４０２ａを廃棄し、それ以降ＳＳＬ通信を行う場合には、サーバ証明書としてＡＰサーバ証明書Ｂを送付する。

【００７１】

このようにＣＡ証明書Ａ１０６ａの有効期限が切れると、クライアント４１５のサーバ認証部４１６は、アプリケーションサーバ４０１との通信にあたり、新しいＡＰサーバ証明書Ｂを受け取ることになる。しかし、メモリ４１８に保存しているＣＡ証明書Ａ１０６ａ内のＣＡ公開鍵Ａでは、ＡＰサーバ証明書Ｂの認証に失敗する。このときサーバ認証部４１６は、予備メモリ４１９に保存されているＣＡ情報Ｂ１０６ｂ内のＣＡ公開鍵Ｂを用いてＡＰサーバ証明書Ｂの認証を行い、ＡＰサーバ証明書Ｂの正当性を確認できると、クライアント４１５はアプリケーションサーバ４０１とのＳＳＬ通信を継続する。

【００７２】

同時に、サーバ認証部４１６は、予備メモリ４１９に保存されているＣＡ情報Ｂ１０６ｂをメモリ４１８に保存し、予備メモリ４１９を空にする。これ以降は、サーバ認証部４１６は、メモリ４１８に保存されたＣＡ情報１０６ｂをアプリケーションサーバ４０１との認証に用いる。

【００７３】

もしこのとき予備メモリ４１９には何も保存されていない場合には、サーバ認証部４１６は、ＣＡ情報更新部４１７に新しいＣＡ情報の取得を指示する。

【００７４】

ＣＡ情報更新部４１７は、サーバ認証部４１６から新しいＣＡ情報の取得を指示された場合には、ダウンロードサーバＢ４０６ｂから新しいＣＡ情報Ｂ３０１

ｂを、上記と同様の手順で取得する。

【００７５】

サーバ認証部４１６は、新しいＣＡ情報Ｂ３０１ｂが取得された後は、上記と同様に、ＣＡ情報Ｂ３０１ｂを用いてアプリケーションサーバ４０１の認証を行う。

【００７６】

以降、ＣＡ証明書の有効期限が近づいたときには、同様の動作を行うことにより、クライアント４１５は自動的に新しいＣＡ証明書を取得できるようになり、またＣＡ証明書の有効期限が切れたときには自動的に新しいＣＡ証明書を用いた認証を行えるようになる。

【００７７】

以上のように、本実施の形態によれば、認証局Ａ１０１ａは、ＣＡ証明書とペアで、次回にＣＡ証明書をダウンロードするためのダウンロードサーバＢ４０６ｂのＵＲＬをクライアント４１５に送付しておく。そして、ＣＡ証明書の有効期限が近づくと、新しいＣＡ証明書を発行する認証局Ｂ１０１ｂを稼働させ、同時に、ダウンロードサーバＢ４０６ｂを稼働させる。一方、クライアント４１５は、定期的にダウンロードサーバＢ４０６ｂのＵＲＬにアクセスを試み、アクセスに成功すれば、新しいＣＡ証明書をダウンロードし、予備メモリ４１９に保存する。そして、通信相手のアプリケーションサーバ４０１のサーバ証明書が現在のＣＡ証明書で認証できなくなった場合には、予備メモリ４１９に保存されている新しいＣＡ証明書で認証し、アプリケーションサーバの正当性を確認できれば、元のＣＡ証明書を削除し、以降は新しいＣＡ証明書をサーバ証明書の認証に使用する。

【００７８】

これによって、クライアント４１５は、次に有効となるＣＡ証明書を保持するだけでＣＡ証明書を更新することができるので、常に多数個のＣＡ証明書を保有したり、複数のＣＡ証明書を用いて検証するプログラムもしくは回路を組み込んでおいたりする必要がない。また、クライアント４１５は、定期的にダウンロードサーバＢ４０６ｂにアクセスして新しいＣＡ証明書を取得することで、新たな

アプリケーションサーバとの通信を開始することができるので、時計を用いてＣＡ証明書の有効期限を監視する必要がない。よって、クライアント４１５は、家電製品などのように十分なリソースを保有していない機器であっても、ＣＡ証明書の有効期限がいつかを気にすることなく、確実にＣＡ証明書の取得および更新を行うことができる。

【００７９】

なお、ＣＡ情報更新部４１７が、メモリ４１８に保存されているＣＡ情報に記載されているＵＲＬが示すダウンロードサーバへの接続は１ヶ月毎に試みるとしたが、１ヶ月ではなくそれより長いもしくは短い期間であってもよい。またその期間は均一であってもよいし、ある程度ばらついていても構わない。要するに、ダウンロードサーバの稼働開始から現在のＣＡ証明書の有効期限が切れる間に確実に１度は接続を試みられる期間であればよい。

【００８０】

またアプリケーションサーバ４０１は、ＣＡ証明書の有効期限が切れると同時に、新しいＡＰサーバ公開鍵とＡＰサーバ秘密鍵の鍵ペアを作成するとしたが、ＣＡ証明書の有効期限内でも新しいＡＰサーバ公開鍵とＡＰサーバ秘密鍵の鍵ペアを作成し、新しいＡＰサーバ証明書を取得してもよい。この場合でも新しいＡＰサーバ証明書には、同じＣＡ秘密鍵によるＡＰ署名が含まれているので、クライアント４１５は保存しているＣＡ公開鍵を用いて新しいＡＰサーバ証明書の認証を行うことができる。

【００８１】

また、図１のＣＡ情報３０１にその他の情報が含まれていても構わない。

【００８２】

また、ＣＡ情報更新部４１７は、ダウンロードした新しいＣＡ情報の正当性が確認できると、新しいＣＡ情報を予備メモリ４１９に保存するが、このときＣＡ署名３０３は保存しなくてもよい。これにより予備メモリ４１９の容量を削減可能となる。

【００８３】

同様に、初期状態としてメモリ４１８にはＣＡ情報Ａ１０６ａが保存されてい

るが、ＣＡ署名Ａ３０３ａは保存しておかなくてもよい。

【００８４】

また、サーバ認証部４１６は、予備メモリ４１９に保存されているＣＡ情報１０６ｂをメモリ４１８に保存し、予備メモリ４１９を空にするとしたが、その代わりにメモリ４１８を空にして、それ以降はメモリ４１８と予備メモリ４１９の役割を交代させるようにし、以降ＣＡ情報の更新を行う毎に、メモリ４１８と予備メモリ４１９の役割を交代させるようにしてもよい。

【００８５】

さらに、本発明のサーバ認証装置の全部または一部の手段の全部または一部の機能をコンピュータにより実行させるためのプログラム及び／またはデータを担持した媒体であって、コンピュータにより処理可能なことを特徴とする媒体も本発明に属する。

【００８６】

さらに、本発明のサーバ認証装置の全部または一部の手段の全部または一部の機能をコンピュータにより実行させるためのプログラム及び／またはデータであることを特徴とする情報集合体も本発明に属する。

【００８７】

（第２の実施の形態）

以下、本発明の第１の実施の形態における認証局およびダウンロードサーバの運用の一例を、本発明の第２の実施の形態として、図３～図７を用いて説明する。

【００８８】

図３は、認証局およびダウンロードサーバの運用例を表すフローチャートである。

【００８９】

図４は、ダウンロードサーバの終了判断を行うフローチャートである。

【００９０】

図５は、正常時の認証局、クライアント、ダウンロードサーバおよびアプリケーションサーバの動作フローの一例である。

【００９１】

図６は、ＣＡ証明書Ａが有効期限前に失効した場合の認証局、クライアント、ダウンロードサーバおよびアプリケーションサーバの動作フローの一例で、失効時に次回ダウンロードサーバが未稼働の場合である。

【００９２】

図７は、ＣＡ証明書Ａが有効期限前に失効した場合の認証局、クライアント、ダウンロードサーバおよびアプリケーションサーバの動作フローの一例で、失効時に次回ダウンロードサーバがすでに稼働している場合である。

【００９３】

本実施の形態においては、ＣＡ情報３０１を発行し、かつアプリケーションサーバ４０１にＡＰサーバ証明書を発行する装置を、認証局と表記する。

【００９４】

また、ＣＡ証明書Ａ１０６ａの有効期限を２０年とし、ＣＡ証明書Ａ１０６ａの有効期限が切れる５年前に新しい認証局Ｂ１０１ｂおよびダウンロードサーバ Ｂ４０６ｂを稼働させるものとする。

【００９５】

またダウンロードサーバは、一つ前のＣＡ証明書に指定されている有効期限が切れる時に稼働を終了させるものとする。例えば、ダウンロードサーバＢ４０６ｂは、ＣＡ証明書Ａ１０６ａに指定されている有効期限、すなわち認証局Ａ１０１ａの稼働開始から２０年後となる。

【００９６】

まず認証局およびダウンロードサーバの運用例を図３および図４のフローチャートを用いて説明する。

【００９７】

図３において、ステップ５０１で運用を開始、ステップ５０２で認証局Ａ１０１ａの稼働を開始する。

【００９８】

ステップ５０３でＣＡ証明書Ａ１０６ａが有効期限前に失効しているかどうかを確認し、失効している場合にはステップ５１１に、失効していない場合にはス

テップ５０４に進む。

【００９９】

ステップ５０４でＣＡ証明書Ａ１０６ａの有効期限が切れる５年前になっているかどうかを確認し、５年前になっていない場合にはステップ５０３に戻り、５年前になった場合にはステップ５０５に進む。

【０１００】

ステップ５０５で認証局Ｂ１０１ｂを仮稼働させ、ステップ５０６でダウンロードサーバＢ４０６ｂを稼働させ、ステップ５０７に進む。この時点では、認証局Ｂ１０１ｂはＣＡ公開鍵ＢとＣＡ秘密鍵Ｂ１０５ｂとの鍵ペアを作成し保有しているが、アプリケーションサーバ４０１がクライアント４１５に送付するサーバ証明書はＡＰサーバ証明書Ａ４０２ａのままである。

【０１０１】

ステップ５０７でＣＡ証明書Ａ１０６ａが有効期限前に失効しているかどうかを確認し、失効している場合にはステップ５０９に、失効していない場合にはステップ５０８に進む。

【０１０２】

ステップ５０８でＣＡ証明書Ａ１０６ａの有効期限が切れているかどうかを確認し、切れていない場合にはステップ５０７に戻り、切れた場合にはステップ５０９に進む。

【０１０３】

ステップ５０９で認証局Ａ１０１ａの稼働を終了させ、ステップ５１０で認証局Ｂ１０１ｂを本稼働させ、ステップ５１２に進む。この時点で、アプリケーションサーバ４０１がクライアント４１５に送付するサーバ証明書は、ＣＡ秘密鍵Ｂ１０５ｂによる署名が付加されたＡＰサーバ証明書Ｂである。

【０１０４】

ステップ５１１ではダウンロードサーバ４０６ｂを稼働させ、ステップ５０９に進む。

【０１０５】

ステップ５１２に進むと、ステップ５０３に戻り、ＡおよびａをＢおよびｂに

、ＢおよびｂをＣおよびｃにそれぞれ置き換えて、ステップ５０３以降の動作を実行する。

【０１０６】

また現在稼働しているダウンロードサーバの稼働を終了させるかどうかは、図４に示すフローチャートで表される。

【０１０７】

ステップ６０１でダウンロードサーバが稼働すると、ステップ６０２でダウンロードサーバの稼働期間を確認し、稼働期間を終了していない場合は、ステップ６０２に戻り稼働期間の終了まで待ち、稼働期間を終了している場合は、ステップ６０３に進む。

【０１０８】

ステップ６０３でダウンロードサーバの稼働を終了し、ステップ６０４で終了する。

【０１０９】

以降、同様の動作を繰り返し、認証局およびダウンロードサーバの稼働と終了を行う。

【０１１０】

以上のように、本実施の形態によれば、ＣＡ証明書が有効期限で終了した場合だけでなく、有効期限前に失効した場合であっても、実施の形態１と同様に、クライアント４１５は、次に有効となるＣＡ証明書を保持するだけでＣＡ証明書を更新することができるので、常に多数個のＣＡ証明書を保有したり、複数のＣＡ証明書を用いて検証するプログラムもしくは回路を組み込んでおいたりする必要がない。また、クライアント４１５は、定期的に、次に有効となるダウンロードサーバにアクセスして新しいＣＡ証明書を取得することで、新たなアプリケーションサーバとの通信を開始することができるので、時計を用いてＣＡ証明書の有効期限を監視する必要がない。よって、クライアント４１５は、家電製品などのように十分なリソースを保有していない機器であっても、ＣＡ証明書の有効期限がいつかを気にすることなく、確実にＣＡ証明書の取得および更新を行うことができる。

【０１１１】

なお図３において、ステップ５０５とステップ５０６の順序は逆でもよいし、全く同時であっても構わない。同様にステップ５０９とステップ５１０の順序は逆でもよいし、全く同時であっても構わない。

【０１１２】

次に図３および図４のフローチャートに従って認証局およびダウンロードサーバの運用を行った場合の、クライアント、ダウンロードサーバおよびアプリケーションサーバの動作フローを、通常時（ＣＡ証明書が有効期限切れにより失効）、および有効期限切れより前に何らかの理由でＣＡ証明書が失効したときのそれぞれの場合について説明する。なお有効期限切れより前に何らかの理由でＣＡ証明書が失効した場合の動作フローは、失効した時点で次のダウンロードサーバが稼働しているときと、稼働していないときの２通りについて説明する。

【０１１３】

図５は通常時のクライアント、ダウンロードサーバおよびアプリケーションサーバの動作フローである。

【０１１４】

初期状態のクライアント４１５においては、メモリ４１８内にはＣＡ情報Ａ３０１ａが保存されているが、予備メモリ４１９には何も保存されていない。

【０１１５】

ＣＡ証明書Ａ１０６ａの有効期限内は、アプリケーションサーバ４０１が送付するＡＰサーバ証明書ＡはＣＡ公開鍵Ａで認証可能であるため、クライアント４１５は自身が保持しているＣＡ情報Ａ３０１ａを用いてアプリケーションサーバ４０１の正当性を確認できる。

【０１１６】

またクライアント４１５は、ＵＲＬ　Ｂ３０２ｂが示すダウンロードサーバＢ４０６ｂへの接続を定期的に試みるが、ＣＡ証明書Ａ１０６ａの有効期限が切れる５年前まではダウンロードサーバＢ４０６ｂはまだ稼働していないため、接続には必ず失敗する。

【０１１７】

ＣＡ証明書Ａ１０６ａの有効期限が残り５年前になった時点で、新しい認証局Ｂ１０１ｂを稼働し、新しいＣＡ証明書Ｂ１０６ｂとＣＡ情報Ｂ３０１ｂが作成される。同時にＣＡ情報Ｂ３０１ｂのダウンロードが可能なダウンロードサーバ４０６ｂを稼働する。

【０１１８】

ダウンロードサーバ４０６ｂが稼働すると、クライアント４１５は、ダウンロードサーバ４０６ｂへの接続に成功し、ＣＡ情報Ｂ３０１ｂを取得することができる。クライアント４１５は、ＣＡ情報Ｂ３０１ｂが正当であることを確認すると、ＣＡ情報Ｂ３０１ｂを予備メモリ４１９に保存する。

【０１１９】

クライアント４１５は、ダウンロードサーバ４０６ｂへの接続を定期的に試みるため、ＣＡ証明書Ａ１０６ａの有効期限が切れる前は、ＣＡ情報Ｂ３０１ｂを取得した後であってもダウンロードサーバ４０６ｂへの接続とＣＡ情報Ｂ３０１ｂの取得は継続される。この場合、予備メモリ４１９内のＣＡ情報と取得したＣＡ情報が同一であれば予備メモリ４１９への保存をしないようにしてもよいし、取得したＣＡ情報が正当なものであれば常に上書きするようにしてもよい。

【０１２０】

さてＣＡ証明書Ａ１０６ａの有効期限が切れると、アプリケーションサーバ４０１は、新しいＣＡ証明書Ｂ１０６ｂで認証するＡＰサーバ証明書Ｂを、サーバ認証に用いるようになる。この後、クライアント４１５がアプリケーションサーバ４０１とのＳＳＬ通信を開始するにあたり取得するサーバ証明書はＡＰサーバ証明書Ｂになるが、保持しているＣＡ証明書Ａ１０６ａではＡＰサーバ証明書Ｂの認証は失敗する。

【０１２１】

すると、クライアント４１５は予備メモリ４１９に保存しているＣＡ情報Ｂ３０１ｂ内のＣＡ証明書Ｂ１０６ｂを用いてＡＰサーバ証明書Ｂの認証を行う。クライアント４１５は、ＡＰサーバ証明書Ｂが正当であると確認すると、ＳＳＬ通信を継続し、同時に予備メモリ４１９内のＣＡ情報Ｂ３０１ｂをメモリ４１８に移し、予備メモリ４１９内の情報は削除する。

【０１２２】

これ以降、クライアント４１５は、ＣＡ証明書Ｂ１０６ｂを用いてサーバ認証を行い、またＣＡ情報Ｂ３０１ｂ内のＵＲＬ　Ｃ３０２ｃで表されるダウンロードサーバＣへの接続を定期的に行うようにする。

【０１２３】

この場合、ダウンロードサーバＢ４０６ｂは、ＣＡ証明書１０６ａが失効すると同時に稼働を終了する。

【０１２４】

以下、同様の動作を継続することにより、認証局およびＣＡ証明書が新しくなった場合でも、クライアント４１５はアプリケーションサーバ４０１の認証やＣＡ証明書の更新を行えるようになる。

【０１２５】

さて、ＣＡ秘密鍵Ａ１０５ａが解読されるなど、ＣＡ秘密鍵Ａ１０５ａの安全性が保証できなくなった場合には、速やかにＣＡ証明書Ａ１０６ａを失効させると同時に、新しい認証局Ｂ１０１ｂを稼働させ、新しいＣＡ証明書Ｂ１０６ｂを発行する。同時にアプリケーションサーバ４０１は、新しい認証局Ｂ１０１ｂから新しいＡＰサーバ証明書Ｂを発行してもらい、サーバ認証に用いるようにしなければならない。

【０１２６】

図６は、次回のＣＡ情報をダウンロードするためのダウンロードサーバが稼働する前に、現在のＣＡ証明書が失効した場合の、クライアント、ダウンロードサーバおよびアプリケーションサーバの動作フローである。

【０１２７】

ＣＡ証明書Ａ１０６ａが失効する前の各動作は、図５と同様である。

【０１２８】

ＣＡ証明書Ａ１０６ａが失効した時点で、認証局Ｂ１０１ｂはまだ稼働していないので、速やかに新しい認証局Ｂ１０１ｂを稼働し、新しいＣＡ証明書Ｂ１０６ｂを発行すると同時に、ＣＡ情報Ｂ３０１ｂを作成する。またこれと同時にダウンロードサーバＢ４０６ｂを稼働させ、ＣＡ情報Ｂ３０１ｂをダウンロードで

きるようにする。

【０１２９】

ＣＡ証明書Ａ１０６ａが失効した後、たまたまクライアント４１５がアプリケーションサーバ４０１のサーバ認証を行う前に、ダウンロードサーバＢ４０６ｂへの接続が成功し、新しいＣＡ情報Ｂ３０１ｂを取得できた場合には、クライアント４１５は通常動作時と同様にＣＡ情報の更新を行うことができる。

【０１３０】

しかしＣＡ情報Ｂ３０１ｂの取得前に、クライアント４１５がアプリケーションサーバ４０１のサーバ認証を行うと、クライアント４１５がＡＰサーバ証明書Ｂの認証に失敗するが、このとき予備メモリ４１９には新しいＣＡ情報Ｂ３０１ｂは保存されていない。この場合、クライアント４１５はただちにダウンロードサーバＢ４０６ｂへの接続を試みる。この時点ではすでにダウンロードＢ４０６ｂが稼働しているので、クライアント４１５はダウンロードＢ４０６ｂから新しいＣＡ情報Ｂ３０１ｂを取得できる。

【０１３１】

新しいＣＡ情報Ｂ３０１ｂを取得した後は、通常時と同様の動作を繰り返す。ただし図６に示すように、ＣＡ証明書Ａ１０６ａが有効期限前に失効した場合でも、ダウンロードサーバＢ４０６ｂは、ＣＡ証明書Ａ１０６ａの本来の有効期限であった時点まで稼働を継続する。

【０１３２】

また図７は、次回のＣＡ情報をダウンロードするためのダウンロードサーバが稼働した後に、現在のＣＡ証明書が失効した場合の、クライアント、ダウンロードサーバおよびアプリケーションサーバの動作フローである。

【０１３３】

ＣＡ証明書Ａ１０６ａが失効する前の各動作は、図５と同様である。

【０１３４】

ＣＡ証明書Ａ１０６ａが失効した時点で、アプリケーションサーバ４０１は新しい認証局Ｂ１０１ｂから発行された新しいＡＰサーバ証明書Ｂを、クライアント４１５とのサーバ認証に使用する。

【０１３５】

またＣＡ証明書Ａ１０６ａが失効した時点で、認証局Ｂ１０１ｂおよびダウンロードサーバＢ４０６ｂは稼働しているので、クライアント４１５はＣＡ情報Ｂ３０１ｂを取得できるようになっている。そのため、クライアント４１５がすでにＣＡ情報Ｂ３０１ｂを取得し、予備メモリ４１９に保存していた場合には、図５と同様に、ＡＰサーバ証明書Ｂの認証に失敗した時点でＣＡ情報の更新を行うことができる。

【０１３６】

またクライアント４１５はＣＡ情報Ｂ３０１ｂを取得する前に、ＡＰサーバ証明書Ｂの認証に失敗した場合には、図６と同様にその時点でダウンロードサーバＢ４０６ｂに接続し、新しいＣＡ情報Ｂ３０１ｂの取得を行い、ＡＰサーバ証明書Ｂの認証を継続する。

【０１３７】

それ以降は、通常時と同様の動作を繰り返す。ただし図７に示すように、ＣＡ証明書Ａ１０６ａが有効期限前に失効した場合でも、ダウンロードサーバＢ４０６ｂは、ＣＡ証明書Ａ１０６ａの本来の有効期限であった時点まで稼働を継続する。

【０１３８】

以下、同様の動作を継続することにより、ＣＡ証明書が有効期限前に失効した場合でも、クライアント４１５はアプリケーションサーバ４０１の認証やＣＡ証明書の更新を行えるようになる。

【０１３９】

なお、ＣＡ証明書の有効期限を２０年、ＣＡ証明書の有効期限が切れる５年前に新しい認証局およびダウンロードサーバを稼働させるとしたが、有効期限は２０年でなくてもよく、また認証局およびダウンロードサーバの稼働開始はＣＡ証明書の有効期限の５年前でなくてもよい。またＣＡ証明書の有効期限は、全て２０年である必要はなく、ＣＡ証明書ごとに異なっていてもよい。

【０１４０】

また、予備メモリ４１９に保存されているＣＡ情報１０６ｂをメモリ４１８に

保存し、予備メモリ４１９を空にするとしたが、その代わりにメモリ４１８を空にして、それ以降はメモリ４１８と予備メモリ４１９の役割を交代させるようにし、以降ＣＡ情報の更新を行う毎に、メモリ４１８と予備メモリ４１９の役割を交代させるようにしてもよい。

【０１４１】

【発明の効果】

以上説明したところから明らかなように、本発明は、リソースの少ない機器でも、ＣＡ証明書の有効期限がいつかを気にすることなく、確実にＣＡ証明書の取得および更新を行うことが可能なサーバ認証装置、認証局およびダウンロードサーバの運用方法、媒体及び情報集合体を容易に提供することができる。

【図面の簡単な説明】

【図１】

第１の実施の形態におけるＣＡ情報の一例を示す図

【図２】

第１の実施の形態におけるサーバ認証を行うクライアントの構成例を示す図

【図３】

第２の実施の形態における認証局およびダウンロードサーバの運用例を表すフローチャート

【図４】

第２の実施の形態におけるダウンロードサーバの終了判断を行うフローチャート

【図５】

第２の実施の形態における認証局、クライアント、ダウンロードサーバおよびアプリケーションサーバの動作フローの一例（正常時）

【図６】

第２の実施の形態における認証局、クライアント、ダウンロードサーバおよびアプリケーションサーバの動作フローの一例（認証局Ｂ稼働前にＣＡ証明書Ａが期限前に失効）

【図７】

第２の実施の形態における認証局、クライアント、ダウンロードサーバおよびアプリケーションサーバの動作フローの一例（認証局Ｂ稼働中にＣＡ証明書Ａが期限前に失効）

【図８】

ＳＳＬにおける鍵情報および証明書の準備を表す図

【図９】

ＳＳＬにおける通信プロトコルを表す図

【符号の説明】

１０１　認証局

１０１ａ　認証局Ａ

１０１ｂ　認証局Ｂ

１０２　クライアント

１０３　サーバ

１０４　ＣＡ公開鍵

１０５　ＣＡ秘密鍵

１０５ａ　ＣＡ秘密鍵Ａ

１０５ｂ　ＣＡ秘密鍵Ｂ

１０６　ＣＡ証明書

１０６ａ　ＣＡ証明書Ａ

１０６ｂ　ＣＡ証明書Ｂ

１０７　サーバ公開鍵

１０８　サーバ秘密鍵

１０９　サーバ証明書

１１０　署名

２０１　通信用共通鍵

３０１　ＣＡ情報

３０１ａ　ＣＡ情報Ａ

３０１ｂ　ＣＡ情報Ｂ

３０２　次回ダウンロードサーバのＵＲＬ

３０２ｂ　ダウンロードサーバＢのＵＲＬ

３０２ｃ　ダウンロードサーバＣのＵＲＬ

３０３　ＣＡ署名

３０３ａ　ＣＡ署名Ａ

３０３ｂ　ＣＡ署名Ｂ

４０１　アプリケーションサーバ

４０２ａ　ＡＰサーバ証明書Ａ

４０３ａ　ＡＰサーバ公開鍵Ａ

４０４ａ　ＡＰサーバ秘密鍵Ａ

４０５ａ　ＡＰ署名Ａ

４０６ｂ　ダウンロードサーバＢ

４０８ｂ　ＤＬサーバ証明書Ｂ

４０９ｂ　ＤＬサーバ公開鍵Ｂ

４１０ｂ　ＤＬサーバ秘密鍵Ｂ

４１２ｂ　ＤＬ署名Ｂ

４１３　ＤＬ秘密鍵

４１４　ＤＬ公開鍵

４１５　クライアント

４１６　サーバ認証部

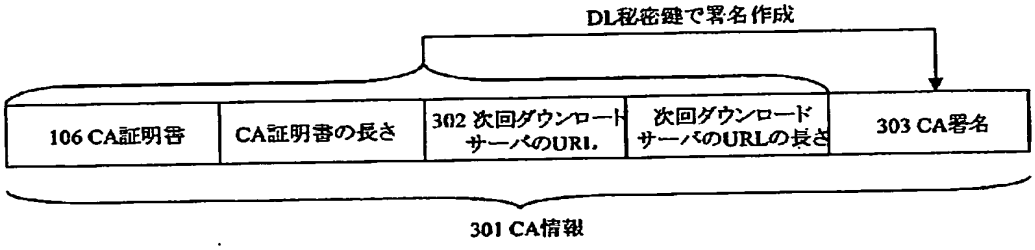
４１７　ＣＡ情報更新部

４１８　メモリ

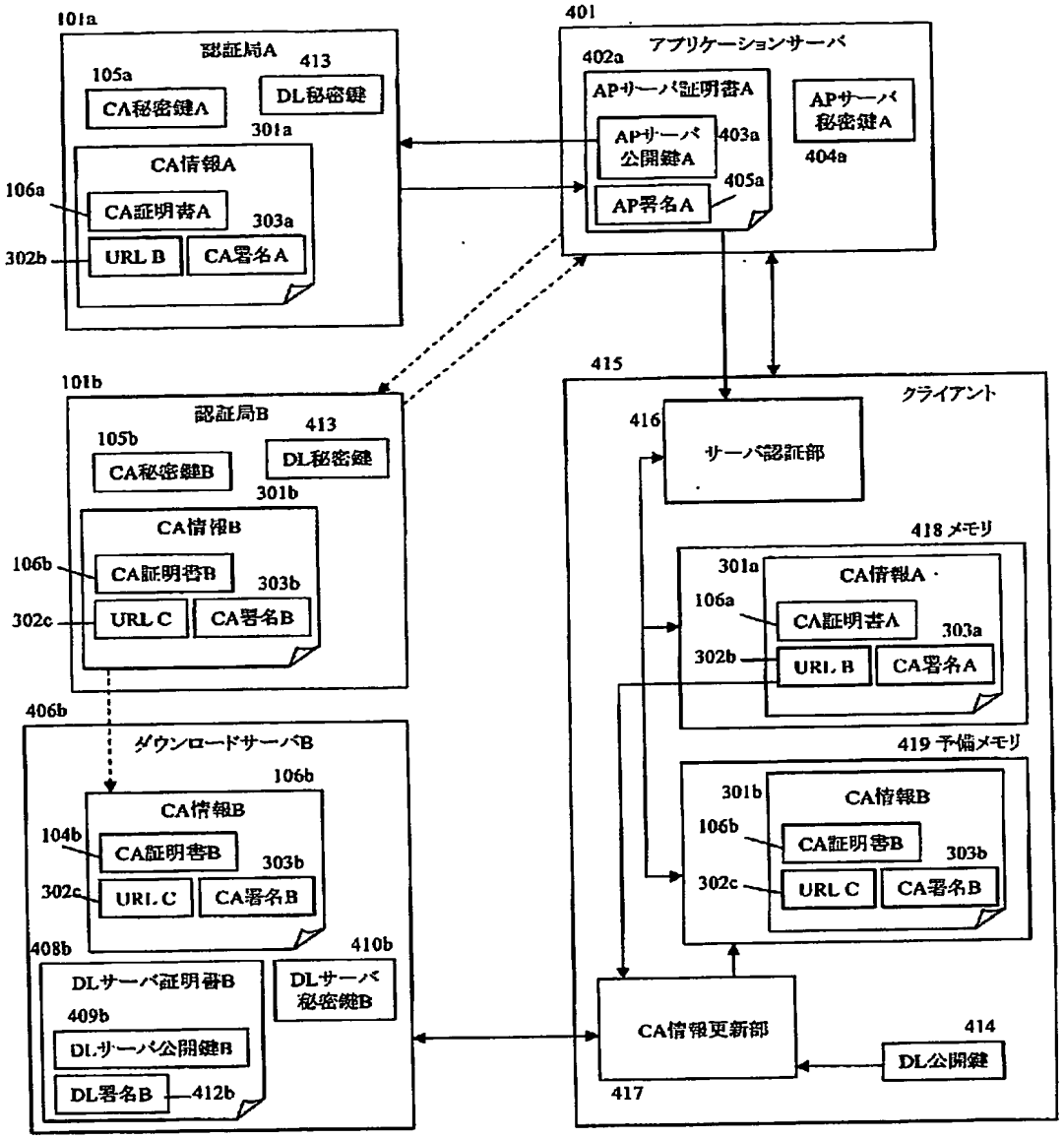
４１９　予備メモリ

【書類名】　図面

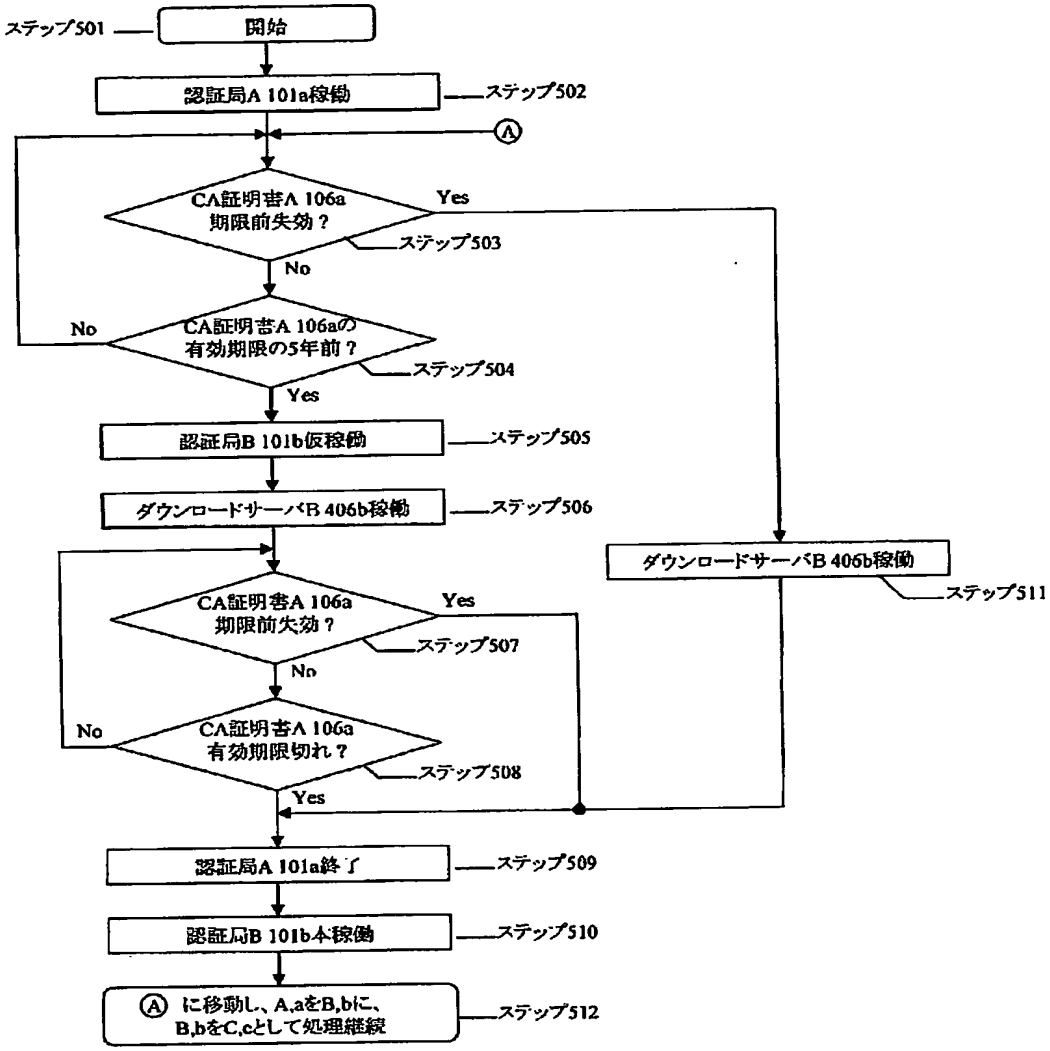
【図１】


DL秘密鍵で署名作成
106 CA証明書
CA証明書の長さ
302 次回ダウンロードサーバのURL
次回ダウンロードサーバのURLの長さ
303 CA署名
301 CA情報

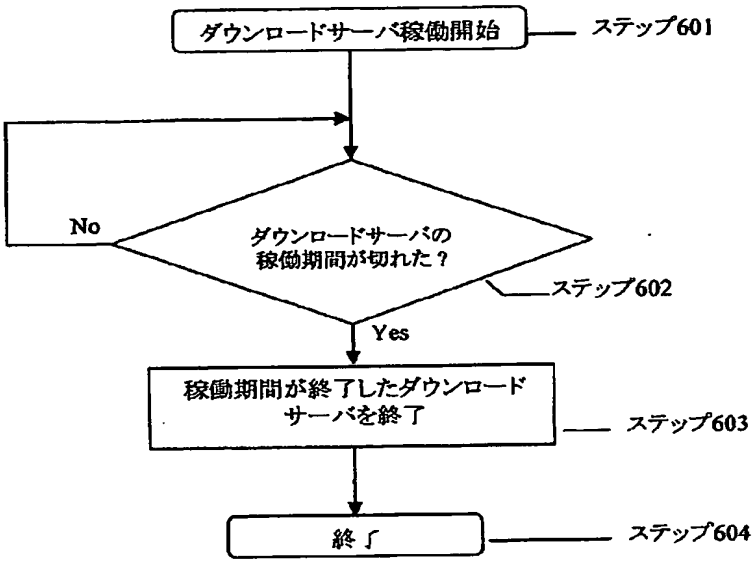
【図２】


101a
認証局A
413
105a
CA秘密鍵A
DL秘密鍵
301a
CA情報A
106a
CA証明書A
303a
302b
URL B
CA署名A
401
アプリケーションサーバ
402a
APサーバ証明書A
APサーバ公開鍵A
403a
APサーバ秘密鍵A
404a
405a
AP署名A
101b
認証局B
413
105b
CA秘密鍵B
DL秘密鍵
301b
CA情報B
106b
CA証明書B
303b
302c
URL C
CA署名B
406b
ダウンロードサーバB
106b
CA情報B
104b
CA証明書B
303b
302c
URL C
CA署名B
408b
410b
DLサーバ証明書B
DLサーバ秘密鍵B
409b
DLサーバ公開鍵B
DL署名B
412b
415
クライアント
416
サーバ認証部
418 メモリ
301a
CA情報A
106a
CA証明書A
303a
302b
URL B
CA署名A
419 予備メモリ
301b
CA情報B
106b
CA証明書B
303b
302c
URL C
CA署名B
CA情報更新部
414
DL公開鍵
417

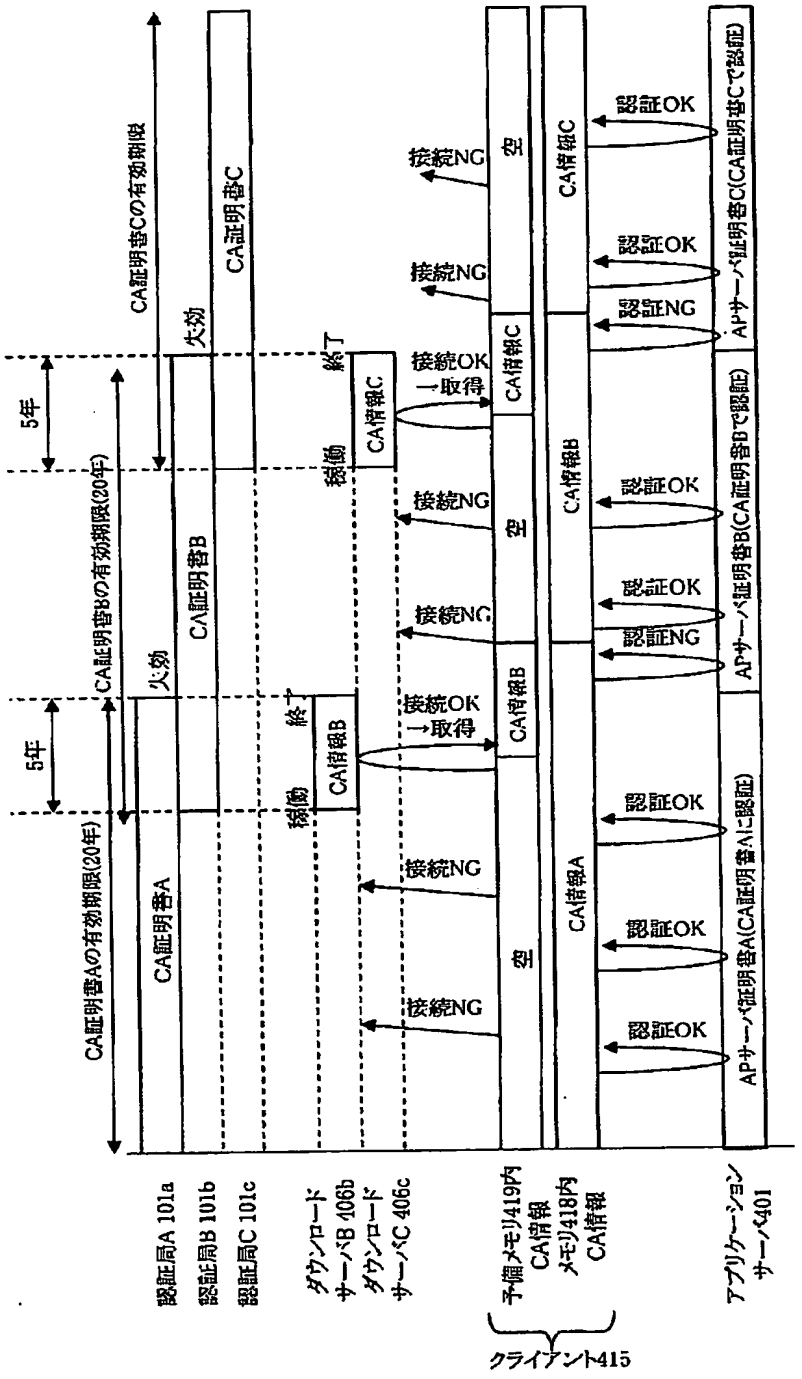
【図３】


ステップ501
開始
認証局A 101a稼働
ステップ502
Ⓐ
CA証明書A 106a
期限前失効？
Yes
ステップ503
No
CA証明書A 106aの
有効期限の5年前？
No
ステップ504
Yes
認証局B 101b仮稼働
ステップ505
ダウンロードサーバB 406b稼働
ステップ506
ダウンロードサーバB 406b稼働
ステップ511
CA証明書A 106a
期限前失効？
Yes
ステップ507
No
CA証明書A 106a
有効期限切れ？
No
ステップ508
Yes
認証局A 101a終了
ステップ509
認証局B 101b本稼働
ステップ510
Ⓐ に移動し、A,aをB,bに、
B,bをC,cとして処理継続
ステップ512

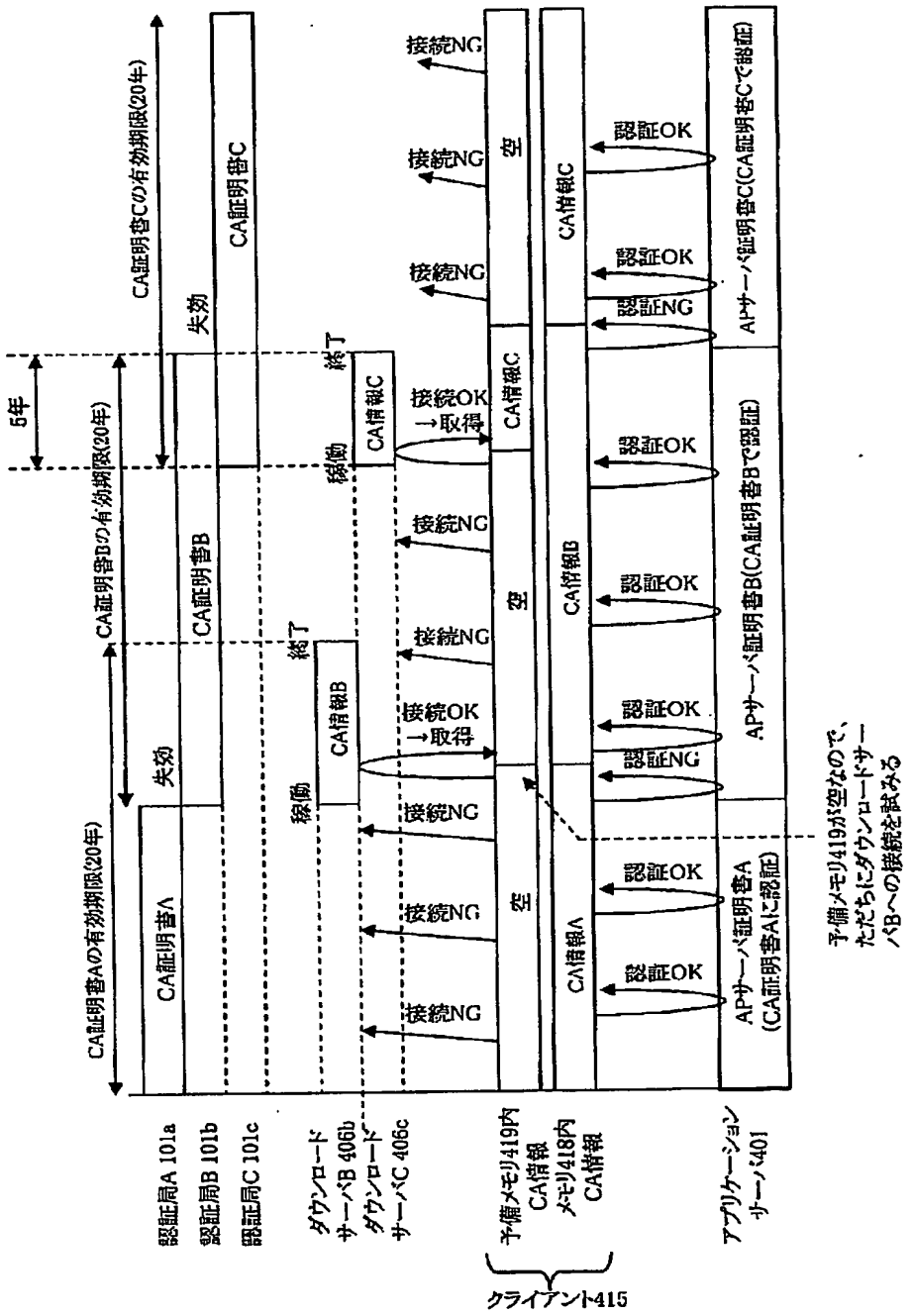
【図４】


ダウンロードサーバ稼働開始
ステップ601
No
ダウンロードサーバの
稼働期間が切れた？
ステップ602
Yes
稼働期間が終了したダウンロード
サーバを終了
ステップ603
終了
ステップ604

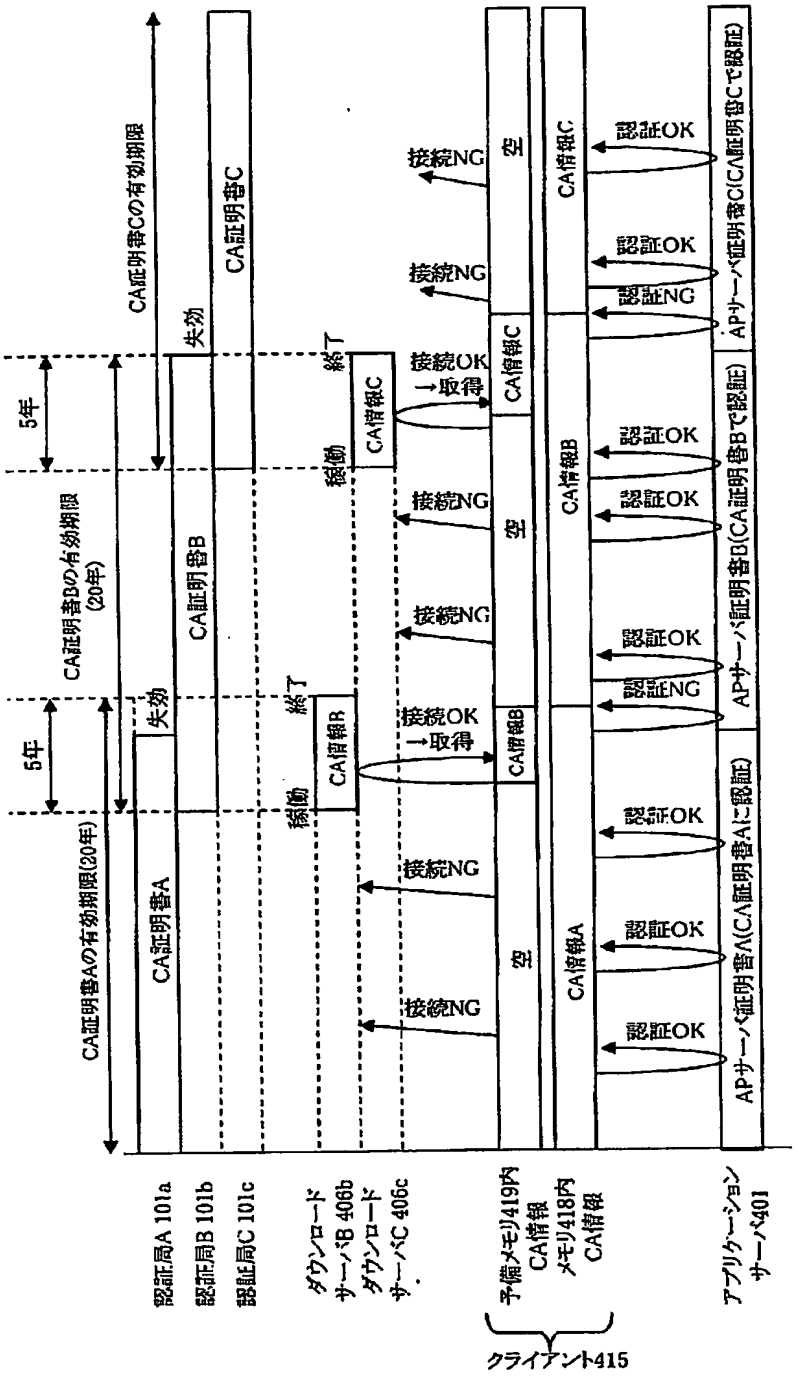
【図５】


CA証明書Cの有効期限
CA証明書Bの有効期限(20年)
CA証明書Aの有効期限(20年)
5年
5年
失効
失効
終了
稼働
終了
稼働
CA証明書A
CA証明書B
CA証明書C
CA情報B
CA情報C
接続NG
接続NG
接続OK
→取得
接続NG
接続NG
接続OK
→取得
接続NG
接続NG
空
空
空
CA情報C
CA情報B
CA情報A
認証OK
認証OK
認証NG
認証OK
認証NG
認証OK
認証OK
APサーバ証明書C(CA証明書Cで認証)
APサーバ証明書B(CA証明書Bで認証)
APサーバ証明書A(CA証明書Aに認証)
認証局A 101a
認証局B 101b
認証局C 101c
ダウンロード
サーバB 406b
ダウンロード
サーバC 406c
予備メモリ419内
CA情報
メモリ418内
CA情報
アプリケーション
サーバ401
クライアント415

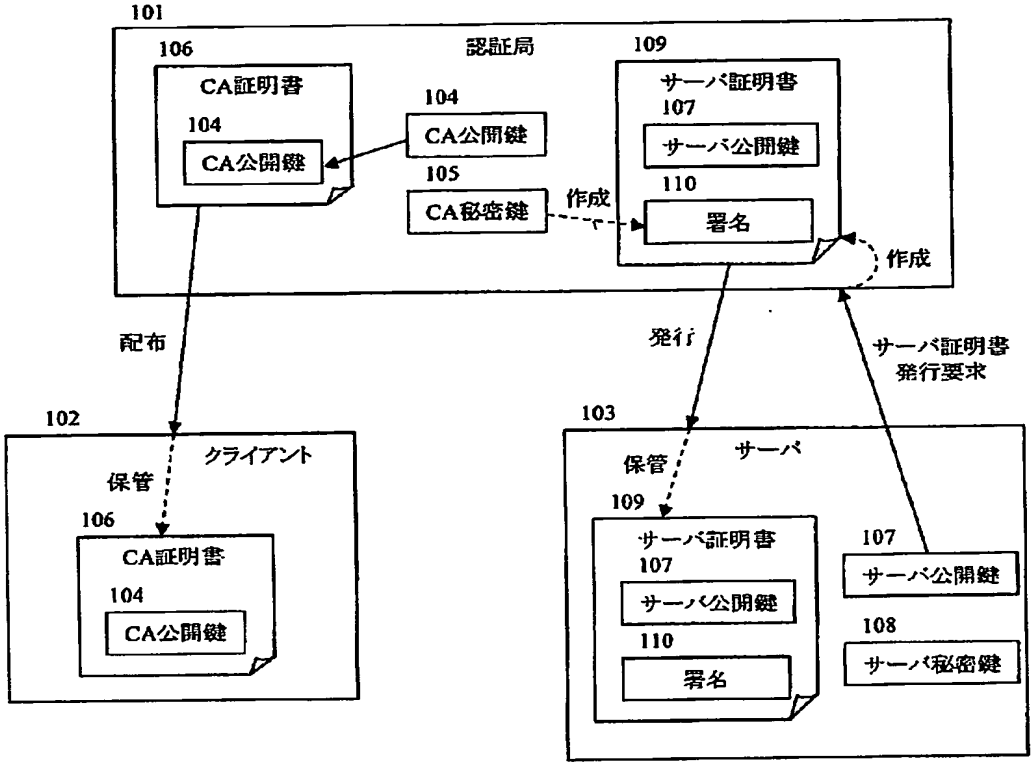
【図６】


CA証明書Cの有効期限(20年)
CA証明書Bの有効期限(20年)
CA証明書Aの有効期限(20年)
5年
失効
CA証明書A
CA証明書B
CA証明書C
稼働
終了
CA情報B
CA情報C
接続NG
接続OK
→取得
認証OK
認証NG
空
CA情報A
CA情報B
CA情報C
APサーバ証明書A
(CA証明書Aに認証)
APサーバ証明書B(CA証明書Bで認証)
APサーバ証明書C(CA証明書Cで認証)
予備メモリ419が空なので、
ただちにダウンロードサー
バBへの接続を試みる
認証局A 101a
認証局B 101b
認証局C 101c
ダウンロード
サーバB 406b
ダウンロード
サーバC 406c
予備メモリ419内
CA情報
メモリ418内
CA情報
アプリケーション
サーバ401
クライアント415

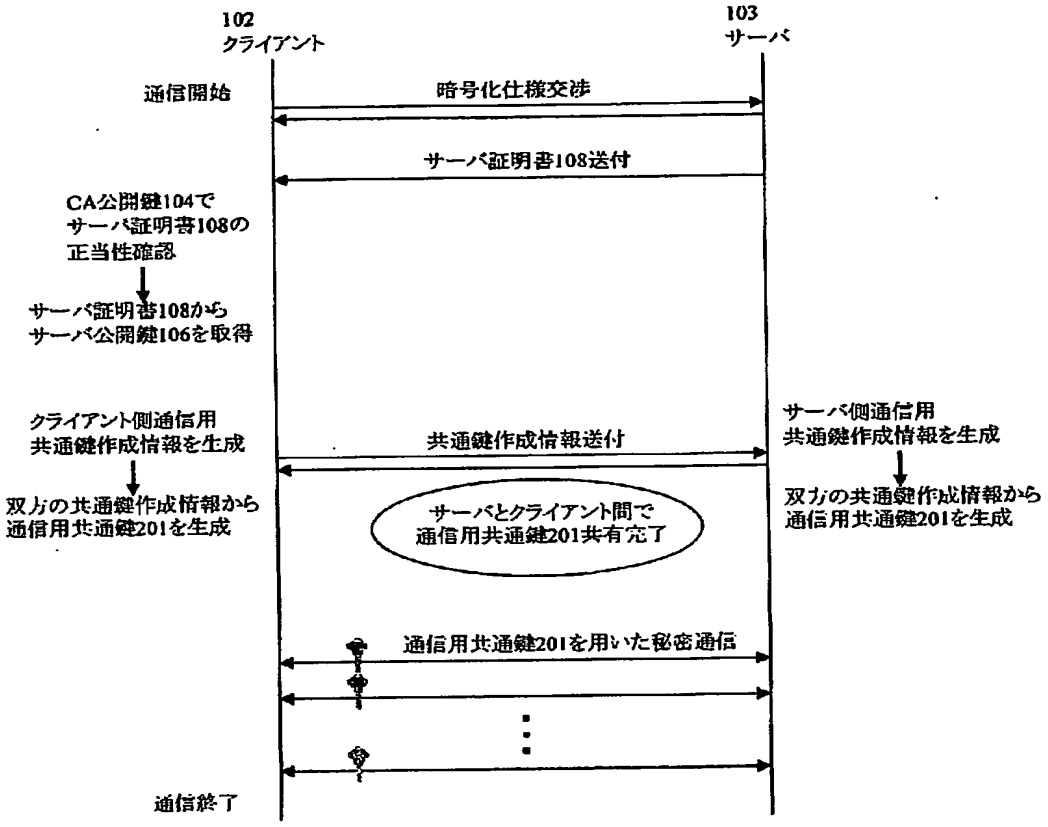
【図７】


CA証明書Cの有効期限
CA証明書Bの有効期限(20年)
CA証明書Aの有効期限(20年)
5年
5年
失効
失効
終了
終了
稼働
稼働
CA証明書A
CA証明書B
CA証明書C
CA情報R
CA情報C
CA情報B
CA情報A
CA情報C
CA情報B
CA情報A
空
空
空
接続NG
接続NG
接続NG
接続NG
接続NG
接続OK
→取得
接続OK
→取得
認証OK
認証NG
認証OK
認証NG
認証OK
認証OK
認証OK
APサーバ証明書C(CA証明書Cで認証)
APサーバ証明書B(CA証明書Bで認証)
APサーバ証明書A(CA証明書Aに認証)
認証局A 101a
認証局B 101b
認証局C 101c
ダウンロード
サーバB 406b
ダウンロード
サーバC 406c
予備メモリ419内
CA情報
メモリ418内
CA情報
クライアント415
アプリケーション
サーバ401

【図８】


101
認証局
106
CA証明書
104
CA公開鍵
104
CA公開鍵
105
CA秘密鍵
作成
109
サーバ証明書
107
サーバ公開鍵
110
署名
作成
配布
発行
サーバ証明書
発行要求
102
クライアント
保管
106
CA証明書
104
CA公開鍵
103
サーバ
保管
109
サーバ証明書
107
サーバ公開鍵
110
署名
107
サーバ公開鍵
108
サーバ秘密鍵

【図９】


102
クライアント
103
サーバ
通信開始
暗号化仕様交渉
サーバ証明書108送付
CA公開鍵104で
サーバ証明書108の
正当性確認
サーバ証明書108から
サーバ公開鍵106を取得
クライアント側通信用
共通鍵作成情報を生成
共通鍵作成情報送付
サーバ側通信用
共通鍵作成情報を生成
双方の共通鍵作成情報から
通信用共通鍵201を生成
サーバとクライアント間で
通信用共通鍵201共有完了
双方の共通鍵作成情報から
通信用共通鍵201を生成
通信用共通鍵201を用いた秘密通信
通信終了

【書類名】　要約書

【要約】

【課題】　リソースの少ないクライアントであっても安全かつ確実に新しいＣＡ証明書を更新することができる認証局等を提供する。

【解決手段】　認証局Ａ１０１ａは、ＣＡ証明書とペアで、次回にＣＡ証明書をダウンロードするためのダウンロードサーバＢ４０６ｂのＵＲＬをクライアント４１５に送付しておく。ＣＡ証明書の有効期限が近づくと、新しいＣＡ証明書を発行する認証局Ｂ１０１ｂを稼働させ、同時に、ダウンロードサーバＢ４０６ｂを稼働させる。クライアント４１５は、定期的にダウンロードサーバＢ４０６ｂのＵＲＬにアクセスを試み、アクセスに成功すれば、新しいＣＡ証明書をダウンロードし、予備メモリ４１９に保存しておき、アプリケーションサーバ４０１のサーバ証明書が現在のＣＡ証明書で認証できなくなった場合に、予備メモリ４１９に保存していた新しいＣＡ証明書で認証する。

【選択図】　図５

認定・付加情報

特許出願の番号	特願２００３－０９８５９６
受付番号	５０３００５４５５０９
書類名	特許願
担当官	第八担当上席　　００９７
作成日	平成１５年　４月　４日

＜認定情報・付加情報＞

【提出日】　平成15年 4月 1日

次頁無

特願２００３－０９８５９６

出願人履歴情報

識別番号　[０００００５８２１]

１．変更年月日　１９９０年　８月２８日
[変更理由]　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社